Правила программы для разработчиков (вступают в силу 12 августа 2020 г.)

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 для более чем 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, для которой оно предназначено.

Нарушение прав ребенка

Категорически запрещается публиковать приложения, в которых несовершеннолетние изображены в сексуальном контексте, в том числе приложения, пропагандирующие педофилию или недопустимые действия в отношении несовершеннолетних (например, ласки или ощупывание).

Также запрещены приложения, предназначенные для детей, но содержащие материалы для взрослых, в том числе те приложения, которые содержат сцены насилия, изображения крови и увечий, а также демонстрируют или поощряют опасные или вредные 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.

Если мы обнаружим такие приложения, то немедленно уберем их из Google Play, сообщим о них в правоохранительные органы и удалим аккаунты всех пользователей, участвовавших в распространении этого контента.

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 сексуального характера, например порнографию и любой контент или услуги, предназначенные для сексуального удовлетворения. Также запрещена непристойная лексика. Мы можем сделать исключение для образовательных, художественных, документальных и научных материалов, содержащих изображение обнаженной натуры, если ее использование оправданно.

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.
- Приложения, содержащие непристойную лексику, в том числе оскорбительные выражения, откровенные тексты, ключевые слова, связанные с сексом или темами, предназначенными только 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, предоставляемых за вознаграждение.
- Приложения, в которых людей унижают или рассматривают как сексуальный объект.

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, пола, возраста, инвалидности, статуса ветерана, сексуальной ориентации, гендерной идентичности и других признаков, которые могут быть причиной систематической дискриминации или маргинализации.

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, издевательства, домогательства, нарушение пищевого поведения, игры с асфиксией и другие действия, которые могут привести к серьезным травмам или смерти.

Материалы террористического характера

Мы не позволяем террористическим организациям публиковать приложения в Google Play ни для каких целей, в том числе для вербовки.

Также нельзя размещать контент, связанный с терроризмом, например пропагандирующий террористическую деятельность, призывающий к насилию и прославляющий теракты. Если такой контент содержится в ваших образовательных, документальных, научных или художественных материалах, сопроводите его необходимыми пояснениями, чтобы пользователи понимали его цель.

Трагические события

Запрещается публиковать приложения, спекулирующие на трагических событиях (природных катаклизмах, случаях проявления жестокости, конфликтах, смерти и т. д.) или выражающие крайнее пренебрежение ими. Приложения, содержащие материалы о трагическом событии, могут быть разрешены. Это касается случаев, когда материалы имеют образовательную, документальную, научную или художественную ценность, либо созданы, чтобы предупредить или проинформировать пользователей о трагическом событии.

Вот примеры наиболее распространенных нарушений:

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

Издевательства и домогательства

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 КБД-масел.

Табачные изделия и алкоголь

Запрещается публиковать приложения, с помощью которых можно приобрести табак (в том числе электронные сигареты и вейпы), а также приложения, поощряющие незаконное или недопустимое потребление алкоголя и табака.

Вот примеры наиболее распространенных нарушений:

- Изображение того, как несовершеннолетние употребляют или приобретают алкоголь и табачные изделия, а также поощрение этого.
- Материалы, подразумевающие, что употребление табака может повысить интеллект или улучшить положение в обществе, сексуальную жизнь или физическую форму.
- Создание положительного образа чрезмерного употребления алкоголя, в том числе запоев и соревнований по распитию спиртного.

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.

Бинарные опционы

Запрещено публиковать приложения, позволяющие пользователям торговать бинарными опционами.

Криптовалюты

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

Потребительские кредиты

Согласно нашим правилам, к потребительским кредитам относятся ссуды, единовременно предоставляемые физическим лицом или организацией отдельному клиенту не для приобретения основных средств или оплаты образования. Вместе с рекламой таких услуг необходимо опубликовать сведения о качестве, характеристиках, комиссии, графиках погашения, рисках и преимуществах кредитных предложений, чтобы пользователи могли принять взвешенное решение.

- Примеры: потребительские кредиты, кредиты наличными, займы между физическими лицами, кредиты под залог автомобиля.
- Не относятся к этой категории: ипотека, кредиты на образование и покупку автомобилей, возобновляемые кредиты (карты, персональные кредитные счета).

Если вы предлагаете потребительские кредиты, в том числе напрямую, осуществляете поиск потенциальных клиентов или помогаете потребителям связаться со сторонними кредиторами, в метаданных приложения необходимо указывать следующую информацию:

- минимальный и максимальный период погашения долга;
- максимальная годовая процентная ставка, в которую обычно включается кредитная ставка, а также комиссии и прочие расходы за год, или же другая похожая ставка, соответствующая действующему законодательству;
- пример расчета общей стоимости займа, включая действующие комиссии;
- политика конфиденциальности, в которой подробно описано, как приложения получают доступ к информации пользователя, какие данные собираются и передаются, а также то, как они используются.

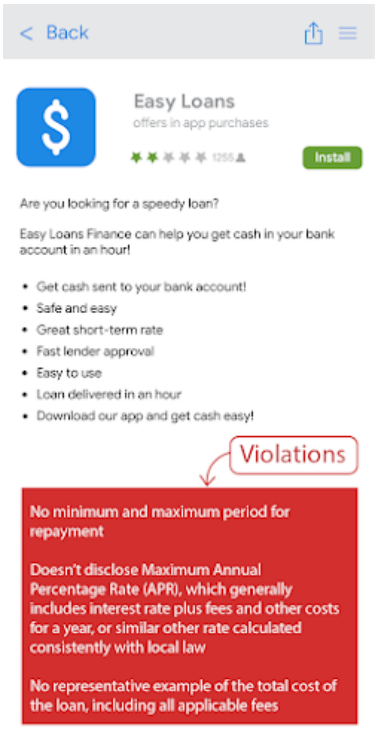
Запрещено публиковать приложения, предлагающие потребительские кредиты, которые необходимо полностью погасить в течение 60 дней после выдачи кредита или быстрее (краткосрочные потребительские кредиты).

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, осуществляют поиск потенциальных клиентов или помогают потребителям связаться со сторонними кредиторами.

Вот пример наиболее распространенного нарушения:



Азартные игры на реальные деньги, игры и соревнования

Приложения и рекламные объявления, связанные с азартными играми на реальные деньги и короткими фэнтези-турнирами, разрешены при условии, что они соответствуют определенным требованиям.

Приложения для азартных игр

(в настоящий момент разрешены только в Великобритании, Ирландии и Франции).
В остальных странах публикация приложений, содержащих контент, связанный с азартными играми, или предлагающих соответствующие услуги, запрещена.

Материалы и сервисы, связанные с азартными онлайн-играми, разрешены при условии, что они соответствуют перечисленным ниже требованиям.

- Разработчик подал заявку и получил разрешение на распространение приложения в Google Play.
- Приложение не нарушает законы и отраслевые стандарты страны, в которой будет распространяться.
- У разработчика есть действующие игровые лицензии для всех стран, где будет распространяться приложение.
- Приложение недоступно для несовершеннолетних пользователей.
- Приложение недоступно для стран, не указанных в игровой лицензии разработчика.
- Приложение распространяется в Google Play бесплатно и НЕ использует функцию оплаты контента через Google Play.
- Приложение можно скачать в Google Play бесплатно.
- Приложению присвоено возрастное ограничение "Только для взрослых" или эквивалентное по рейтингу IARC.
- В приложении и на его странице в Google Play присутствует описание принципов ответственной игры.

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

Запрещено публиковать контент и сервисы, которые позволяют пользователю заключать пари, делать ставки или иным образом использовать реальные деньги (включая покупки в приложении) в борьбе за приз, который имеет реальную денежную стоимость, а также способствуют этим действиям. Это касается в том числе онлайн-казино, спортивных тотализаторов и лотерей, не соответствующих приведенным выше требованиям, а также игр, где выигрышем являются денежные и другие ценные призы.

Вот примеры наиболее распространенных нарушений:

- Игры, где принимаются деньги в обмен на возможность выиграть денежный или иной материальный приз.

- Игры с баллами "лояльности" (например, за вовлеченность или активность), которые можно получить, делая покупки за реальные деньги; или обменять на предметы или призы, имеющие материальную ценность.
- Приложения, которые принимают ставки и взносы во внутренней валюте, необходимые для участия или победы, а также берут залог в обмен на возможность выиграть денежный или иной материальный приз.
- Приложения, которые призывают делать ставки, заключать пари, участвовать в играх на реальные деньги, в том числе конкурсах и турнирах. В частности приложения, где элементы навигации (пункты меню, вкладки, кнопки и т. д.) вида "ЗАРЕГИСТРИРУЙТЕСЬ!" или "ПРИМИТЕ УЧАСТИЕ!" приглашают пользователей посоревноваться за денежный приз.

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

Реклама, связанная с азартными онлайн-играми, а также играми, конкурсами и турнирами на реальные деньги, разрешена при условии, что она соответствует перечисленным ниже требованиям.

- Приложение, объявление и рекламодатель не нарушают законы и отраслевые стандарты страны, в которой объявление будет показываться.
- Объявление соответствует местным требованиям к лицензированию продуктов и услуг, связанных с азартными играми.
- Приложение не показывает рекламу азартных игр лицам заведомо младше 18 лет.
- Приложение не входит в программу "Приложения для всей семьи".
- Лица младше 18 лет не являются целевой аудиторией приложения.
- На целевой странице объявления, в описании приложения в Google Play или в самом приложении содержатся 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 турнирами на реальные деньги (например, не помогает делать ставки, выводить выигрыши, отслеживать счет и котировки или управлять игровыми фондами).
- Вы не имеете доли в праве собственности на игровые сервисы, рекламируемые в приложении.
- Приложение не продвигает азартные игры на реальные деньги и связанные с ними сервисы.

Реклама азартных игр, а также игр, конкурсов и турниров на реальные деньги может демонстрироваться только в приложениях для азартных игр (определение приведено выше) или в приложениях, соответствующих всем требованиям к рекламе азартных игр.

Вот примеры наиболее распространенных 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.
- Новостное приложение, где показывается реклама сервиса азартных игр, принадлежащего разработчику приложения или управляемого им.
- Приложения, содержащие рекламу азартных игр, которая нарушает правила об объявлениях, вводящих в заблуждение, например рекламные объявления, которые выглядят как кнопки, значки или иные интерактивные элементы.

Приложения для коротких фэнтези-турниров

Разрешены приложения для коротких фэнтези-турниров, соответствующие действующим требованиям местного законодательства, если выполняются перечисленные ниже условия.

- Приложение или 1) распространяется исключительно в США; или 2) соответствует приведенным выше требованиям к приложениям для азартных игр.
- 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 совершать денежные транзакции в приложении недоступна для несовершеннолетних.
- Приложение распространяется в Google Play бесплатно и НЕ использует функцию оплаты контента через Google Play.
- Приложение можно скачать в Google Play бесплатно.
- Приложению присвоено возрастное ограничение "Только для взрослых" или эквивалентное по рейтингу IARC.

- В приложении и на его странице в Google Play присутствует описание принципов ответственной игры.

Если приложение распространяется в США, оно должно соответствовать следующим дополнительным требованиям:

- Приложение не нарушает действующие законы и отраслевые стандарты тех штатов или территорий США, где 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:

- Реклама и продажа без рецепта препаратов, продаваемых только по рецепту, или запрещенных наркотических веществ.
- Изображение того, как несовершеннолетние используют или приобретают наркотики, алкоголь и табачные изделия, а также поощрение этого.
- Инструкции по производству запрещенных наркотических веществ, в том числе по выращиванию наркотических растений.

Контент, создаваемый пользователями

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

Приложения, которые содержат создаваемый пользователями контент, должны соответствовать перечисленным ниже требованиям.

- Перед созданием контента и загрузкой пользовательских материалов в приложении необходимо принять условия или правила использования этого приложения.
- Вы должны дать определение неприемлемого контента и поведения, а также объяснить, что такие материалы запрещены. Эта информация должна соответствовать правилам программы для разработчиков и присутствовать в условиях или правилах использования приложения.
- Создаваемый пользователями контент оперативно и регулярно модерируется настолько, насколько это уместно для данного типа материалов.
  - Если пользовательский контент транслируется, то неприемлемые материалы должны удаляться из приложения как можно скорее.
  - При модерации пользовательского контента в приложениях с дополненной реальностью (включая систему отчетов в приложении) необходимо обращать внимание как на сам неприемлемый пользовательский контент в дополненной реальности (например, на изображения сексуального характера), так и на место, к которому он привязан (иногда контент дополненной реальности привязан к территории с ограниченным доступом, например военной базе или объекту частной собственности, и может вызвать проблемы для собственника).
- В приложении можно без труда сообщать о неприемлемом пользовательском контенте и удалять его.
- Разработчик удаляет или блокирует аккаунты пользователей, оскорбляющих других людей и нарушающих условия или правила использования приложения.
- Разработчик принял меры предосторожности для того, чтобы монетизация в приложении не способствовала нежелательному поведению пользователей.

Мы удаляем из Google Play приложения, предназначенные в основном для неприемлемых пользовательских материалов. Так же мы поступаем с приложениями, в которых размещают главным образом неподобающий контент или которые известны наличием таких материалов.

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.

Запрещенные вещества

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

- 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 отпускаемыми по рецепту 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.

Интеллектуальная собственность

Когда разработчик копирует чужую работу или использует ее без необходимого разрешения, это может повредить владельцу информации. Призываем вас отказаться от плагиата 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 вы считаете, 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 соответствующую жалобу 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 контента, защищенного авторским правом, который часто используется без разрешения или юридического основания:

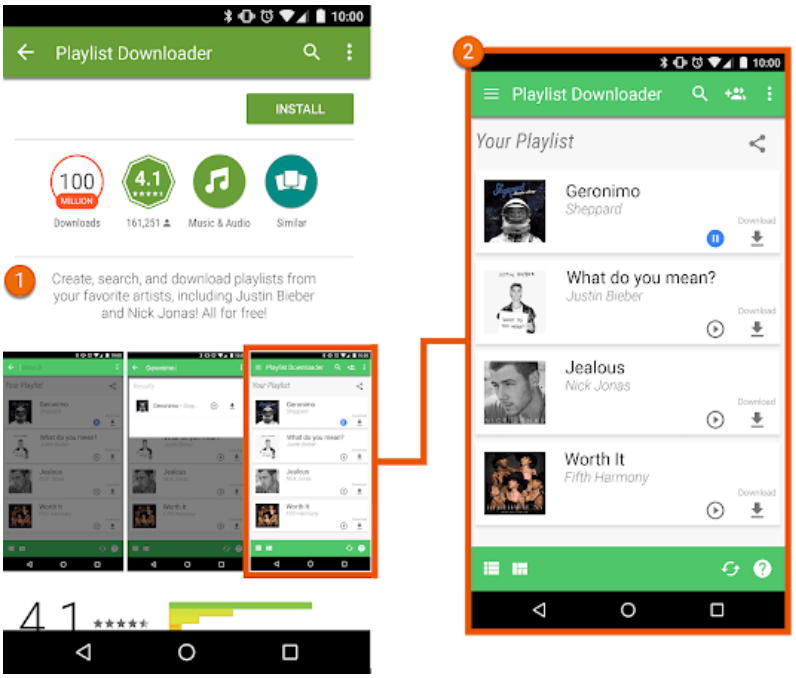
- Обложки музыкальных альбомов, видеоигр и книг.
- Рекламные изображения из фильмов, сериалов, телепередач или видеоигр.
- Изображения или заставки из комиксов, мультфильмов, фильмов, видеоклипов, сериалов или телепередач.
- Логотипы университетских или профессиональных спортивных команд.
- Фотографии 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 нелегально скачивать контент, защищенный авторским правом.
② Скриншот в описании этого приложения призывает пользователей нелегально скачивать контент, защищенный авторским правом.

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

К данным пользователя относятся сведения о нем, а также предоставленные им самим, в том числе информация об устройстве. Обязательно сообщите, как и для чего вы будете использовать и собирать данные, а также получать и предоставлять к ним доступ. Применять информацию в целях, о которых вы не заявили, запрещено. Если ваше приложение обрабатывает личные или конфиденциальные данные, оно должно соответствовать требованиям, перечисленным в разделе "Личная и конфиденциальная информация". Эти правила Google Play дополняют требования действующего законодательства о конфиденциальности и защите данных.

Личная и конфиденциальная информация

К личной и конфиденциальной информации пользователя относятся в том числе сведения, позволяющие идентифицировать личность, финансовые, платежные, учетные и контактные данные (включая телефонную книгу, данные звонков и SMS), данные о местоположении устройства, данные микрофона и камеры, а также другая конфиденциальная информация об устройстве или его использовании. Если ваше приложение обрабатывает личные или конфиденциальные данные, оно должно соответствовать перечисленным ниже требованиям.

- Доступ к личным и конфиденциальным данным, полученным через приложение, а также их сбор, использование и передача допускаются только для предоставления или улучшения функций (например, для обеспечения возможностей, указанных на странице приложения в Google Play). Если вы планируете использовать эти данные также для показа рекламы, ваши приложения должны соответствовать Правилам размещения рекламы.
- Политика конфиденциальности должна быть приведена в предназначенном для нее поле в Play Console и в самом приложении. В политике конфиденциальности и в информации об использовании личных данных в самом приложении необходимо объяснить, какие данные собираются и передаются, а также как они используются. Кроме того, в политике конфиденциальности нужно указать, кто и при каких обстоятельствах может получить доступ к личной и конфиденциальной информации.
- Обрабатывать все личные и конфиденциальные данные пользователя необходимо 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 (когда появится возможность).
- Продавать личную и конфиденциальную информацию запрещено.

Раскрытие информации и разрешение на использование данных

Если у пользователей нет разумных оснований ожидать, что их личные и конфиденциальные данные будут применяться для предоставления и улучшения функций приложения, соответствующих правилам (например, когда их данные собираются в фоновом режиме), необходимо соблюдать перечисленные ниже требования.

В приложении должна содержаться информация о сборе, использовании и передаче личных данных, соответствующая следующим требованиям:

- 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.
- Кроме того, должно быть описано, как именно приложение использует и передает данные.
- **Нельзя** публиковать эту информацию только в политике конфиденциальности и условиях использования.
- **Нельзя** включать эту информацию в документы, которые не имеют отношения к сбору личных и конфиденциальных данных.

Показав эту информацию пользователю, необходимо сразу запросить у него согласие и, когда появится возможность, динамическое разрешение. Использовать или собирать личную и конфиденциальную информацию без согласия ее владельца нельзя. Запрос составляется в соответствии со следующими правилами:

- Запрос нужно сформулировать предельно ясно и показать в диалоговом окне.
- Необходимо попросить пользователя подтвердить разрешение (например, нажать кнопку или установить флажок).
- **Нельзя** считать согласием ситуации, когда пользователь намеренно или случайно закрывает окно с запросом.
- **Запрос** не должен автоматически закрываться или исчезать до того, как пользователь его примет или отклонит.

Вот примеры наиболее распространенных нарушений:

- Приложение получает доступ к списку установленных приложений 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 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 будут использоваться, и не получая согласие пользователя в соответствии с приведенными выше требованиями.
- Приложение собирает ограниченные разрешения в фоновом режиме и использует их в том числе в исследовательских или маркетинговых целях или в целях отслеживания, не раскрывая, для чего они будут использоваться, и не получая согласие пользователя в соответствии с приведенными выше требованиями.

Ограничения доступа к конфиденциальной информации

Ниже перечислены дополнительные требования к приложениям, выполняющим определенные функции.

Действия	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 прочие идентификационные данные.
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.

EU-U.S. Privacy Shield (соглашение о правилах передачи персональных данных между ЕС и США)

Требования

Если вы получаете доступ к личным данным пользователей, предоставленным компанией Google и созданным на территории Европейского союза или Швейцарии, если используете либо обрабатываете эту информацию и по ней можно прямо или косвенно установить личность человека, то вы должны:

- Соблюдать все действующие законы, директивы и правила в отношении конфиденциальности, безопасности и защиты личных данных.
- Получать доступ к личным данным и использовать их только в тех целях, с которыми согласился их владелец.
- Использовать необходимые организационные и технические средства для защиты личных данных от потери, недопустимого использования, несанкционированного или незаконного доступа, разглашения, изменения и

нарушения целостности.
- Обеспечивать личным данным необходимую защиту в соответствии с принципами соглашения Privacy Shield.

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 прекратите обработку личных данных или как можно скорее восстановите их защиту.

Разрешения

Пользователю должно быть понятно, для чего вам требуется то или иное разрешение. Запрашивать разрешения 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, предоставляющие доступ к данным пользователя или устройства, для не заявленных, не внедренных или запрещенных функций или целей. Ни при каких обстоятельствах нельзя продавать личные или конфиденциальные данные, полученные с разрешения пользователя.

Запрашивайте доступ к данным в контексте (с помощью поэтапной авторизации). Это поможет пользователям понять, для чего вам нужно то или иное разрешение. 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

Помимо перечисленных выше, к разрешениям, которые обозначены в документации для разработчиков как опасные, специальные или требующие определенной подписи, применяются дополнительные требования и ограничения.

- Конфиденциальные данные пользователя или устройства, полученные в рамках таких разрешений, можно передавать третьим лицам только в том случае, если это нужно для работы или улучшения уже внедренных функций и сервисов приложения, в котором эти данные получены. Также передача данных возможна, если этого требует действующее законодательство или сделка по слиянию, поглощению компании или продаже активов. Вы должны уведомить об этом пользователя юридически приемлемым способом. Во всех остальных случаях продажа и передача данных пользователя запрещена.
- 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 также обязаны приложить разумные усилия для того, чтобы все равно обеспечить пользователю доступ к функциям приложения (например, предусмотреть возможность ввода телефонного номера вручную, если пользователь запретил доступ к списку вызовов).

В отношении 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
В манифесте приложения содержится требование группы разрешений для списка вызовов (например, READ_CALL_LOG, WRITE_CALL_LOG, PROCESS_OUTGOING_CALLS)	Приложение должно быть зарегистрировано как помощник или обработчик звонков по умолчанию.
В манифесте приложения содержится требование группы разрешений для SMS (например, READ_SMS, SEND_SMS, WRITE_SMS, RECEIVE_SMS, RECEIVE_WAP_PUSH, RECEIVE_MMS)	Приложение должно быть зарегистрировано как обработчик действий Ассистента 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 по умолчанию для SMS или звонков. 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 раздела Личная и конфиденциальная информация, а также следующие требования:

- Приложения не должны использовать сведения, защищенные разрешениями на доступ к данным о местоположении (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). Важно, чтобы доступ действительно требовался для работы сервиса или функции, имеющихся в приложении, и 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.
- Данные о местоположении 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 (например, 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.

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 (Android 11, API уровня 30) 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.

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 рекомендациях по обеспечению качества.

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 и имеет ограниченный доступ к API Android (например, код JavaScript в компоненте WebView или браузере).

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:

- Приложения, которые блокируют или прерывают работу других приложений показом рекламы.
- Приложения, которые влияют на геймплей в играх, например позволяют жульничать.
- Приложения, которые помогают совершать хакерские атаки на сервисы, программы и устройства или обходить системы безопасности, а также предоставляют соответствующие инструкции.
- Приложения, которые нарушают условия использования сервисов или API.
- Приложения, которые пытаются обойти систему управления питанием и при этом не входят в белый список.
- Приложения, которые предоставляют услуги прокси-сервера третьим лицам. Это возможно только в том случае, если услуги прокси-сервера являются ключевой функцией приложения.
- Приложения или сторонний код (например, SDK), которые скачивают исполняемый код (например, файлы DEX или нативный код), созданный сторонними разработчиками.
- Приложения, которые устанавливают на устройство другие приложения без разрешения пользователя.
- Приложения, которые перенаправляют пользователя на сайт с вредоносным ПО или способствуют его распространению и установке.

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.

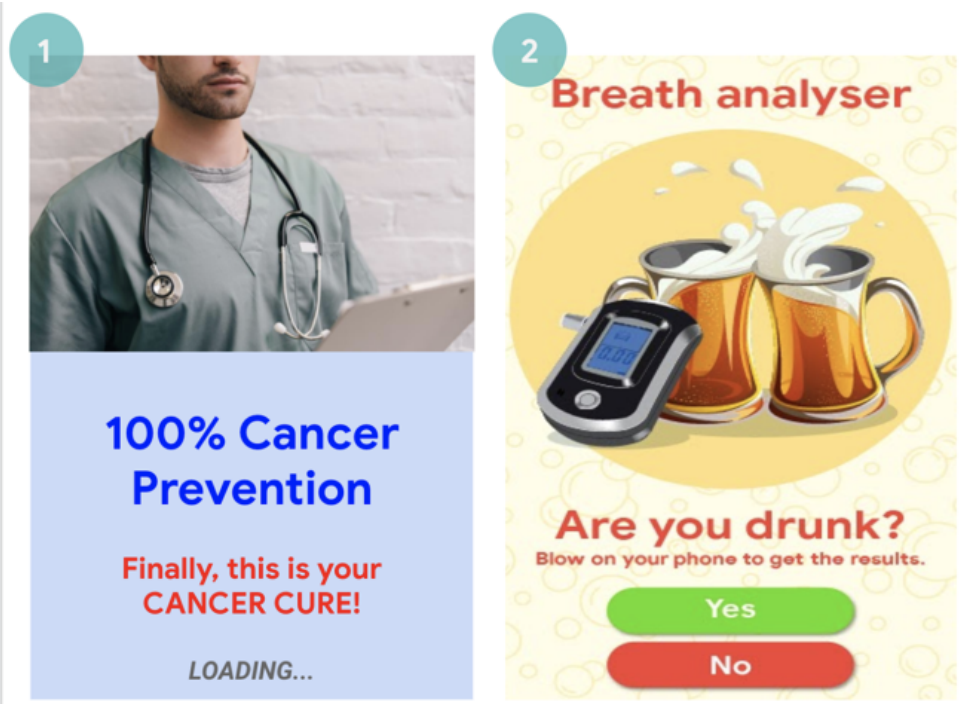
Заявления, вводящие в заблуждение

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.
  - По описанию приложение является антивирусом, хотя всего лишь содержит рекомендации о том, как удалять вирусы.
- Название разработчика или приложения содержит ложные сведения о статусе в Google Play: "Выбор редакции", "Номер 1", "Топ платных" и т. д.
- Приложение содержит сведения о здоровье или медицинскую информацию, которые вводят в заблуждение или являются потенциально опасными.
- В описании приложения указаны невыполнимые функции (например, отпугивание насекомых), даже если это представлено как шутка, розыгрыш или пранк.
- Приложение отнесено к неправильной категории или возрастной группе.
- Явно недостоверный контент, который может повлиять на процесс голосования.
- В описании приложения содержатся ложные заявления о том, что оно связано с государственными органами либо предоставляет государственные услуги или оказывает содействие в их получении, при этом приложение не имеет соответствующих законных полномочий.
- Приложения, которые ложно представлены как официальные продукты другой компании. Запрещается использовать такие названия, как "От Димы Билана", "Официально от Димы Билана" и подобные, без

соответствующих прав.



1) В этом приложении содержатся заявления медицинского характера (лекарство от рака), которые вводят в заблуждение.
2) Для этих приложений заявлены невозможные функции (использование телефона для взятия проб на алкоголь).

Несанкционированные изменения настроек устройства

Запрещено 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 или вынуждают пользователей удалять или отключать программы других разработчиков или 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 и водительских прав. Информация о приложении, его название, описание, а также изображения и видеоролики должны соответствовать его функциональности 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 сообщить пользователю размер этих файлов до того, как начать скачивание.

Заявления о том, что приложение создано для розыгрыша или с другими несерьезными намерениями, не избавляет 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.

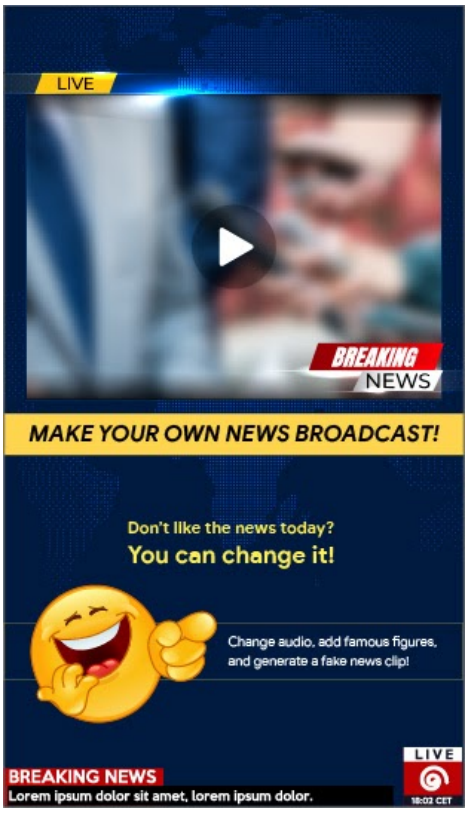
Манипулирование материалами СМИ

Запрещается публиковать приложения, которые способствуют распространению ложной или вводящей в заблуждение информации в виде изображений, видео или текста. Мы не публикуем приложения, содержащие текст, фото или видео, которые демонстративно вводят пользователей в заблуждение и могут представлять угрозу для важных мероприятий, политической сферы, социальных вопросов и других общественно значимых тем.

Если приложение манипулирует материалами СМИ или изменяет содержащуюся в них информацию, нарушая сложившиеся стандарты в отношении качества и ясности, вы должны в явном виде сообщить об этом или отметить измененный контент водяным знаком (когда пользователь может не понять, что материалы были изменены). Исключения могут быть сделаны для тем, представляющих общественный интерес, а также очевидных примеров сатиры или пародии.

Вот примеры наиболее распространенных нарушений:

- Приложения, которые добавляют изображения известных людей на снимки демонстраций во время важных политических событий.
- Приложения, на страницах которых в Google Play используются изображения известных людей или материалы, касающиеся важных событий, для демонстрации функций, позволяющих изменять контент СМИ.
- Приложения, которые изменяют видеоклипы, имитируя выпуски новостей.



1) Это приложение изменяет видеоклипы, имитируя выпуски новостей, а также добавляет в клипы изображения знаменитостей или общественных деятелей без водяного знака.

Искажение фактов

Запрещены приложения и аккаунты разработчиков, выдающие себя за других лиц или другие организации, а также скрывающие или искажающие свою основную цель или сведения о владельцах. Также не допускаются приложения и аккаунты, которые намеренно вводят пользователей в заблуждение, например скрывают или искажают информацию о стране происхождения или предоставляют контент пользователям в других странах.

Вредоносное ПО

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, фишинг и шпионское ПО. Мы постоянно обновляем этот список и добавляем новые категории.

Вредоносное ПО

В основе нашей политики лежит простое правило: экосистема Android, включающая Google Play Маркет и устройства пользователей, не должна подвергаться воздействию вредоносного ПО. Руководствуясь этим принципом, мы стараемся делать экосистему Android безопасной для пользователей и их устройств на базе Android.

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

- нарушение целостности 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.

Некоторые приложения, исполняемые файлы и модификации фреймворков, которые 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.

Более 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-мошенничество, телефонное мошенничество и 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.

Телефонное мошенничество

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 платными звонками. Примеры: оплата через оператора связи, использование беспроводной точки доступа (WAP) и передача минут мобильной связи. Мошенничество с WAP особенно популярно. 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.

Приложения для сталкинга

Код, который передает личную информацию с устройства без согласия пользователя, а также не показывает уведомление, когда происходит отправка этой информации.

Приложения для сталкинга передают данные третьим лицам (тем, кто не является поставщиком этого ПО). Родители не могут использовать легальные приложения такого рода, чтобы отслеживать действия своих детей. Однако с помощью этих приложений также можно следить за человеком (например, супругом или супругой) без его согласия – если при передаче данных на экране не будет уведомления, пользователь не узнает, что его информация кому-то отправляется.

Единственные приложения с функциями отслеживания и отправки отчетов, которые могут быть опубликованы в Google Play, – это приложения, предназначенные для родительского или корпоративного контроля. При этом они должны полностью соответствовать всем перечисленным ниже правилам и требованиям.

Опубликованные в Google Play приложения, которые отслеживают действия пользователя на устройстве, должны соответствовать перечисленным ниже требованиям.

- В описании приложения не должно говориться, что это шпионское ПО или решение для секретной слежки.
- Приложения не должны скрывать свои функции отслеживания или вводить пользователя в заблуждение по этому поводу.
- Во время работы таких приложений должно постоянно отображаться уведомление с уникальным значком.
- В приложениях и на их страницах в Google Play не должно быть способов активировать функции, нарушающие данные правила, или получить доступ к таким функциям. Например, запрещены ссылки на не соответствующие требованиям APK-файлы, размещенные не в Google Play.
- Вы несете полную ответственность за соответствие вашего приложения законам страны, где оно будет распространяться. Приложения, нарушающие местное законодательство, подлежат удалению.

Атака типа "отказ в обслуживании" (DoS)

Код, который незаметно для пользователя запускает атаку типа "отказ в обслуживании" (DoS) или является частью распределенной атаки 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 банковских 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 определенные действия.

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

Код, который передает личные данные с устройства без уведомления и согласия пользователя.

Например, признаком шпионского ПО считается передача без ведома пользователя следующей информации:

- списка контактов;
- фотографий и других файлов с SD-карты, а также файлов, которые не принадлежат приложению;
- писем пользователя;
- списка вызовов;
- списка SMS;
- истории веб-поиска или закладок в используемом по умолчанию браузере;
- информации из каталогов /data/ других приложений.

Шпионским также может считаться ПО, которое следит за пользователем, например записывает аудио и входящие звонки или крадет данные приложений.

Трояны

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 их 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.

Однако 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.

Нежелательное ПО для мобильных устройств

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.

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

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;
- выдача себя за другое лицо.

Защита пользовательских данных

Явным образом сообщите, как приложения получают доступ к информации пользователя, какие данные собираются и передаются, как они используются. Пользовательская информация должна использоваться в соответствии со всеми действующими правилами. При работе с ней необходимо принимать меры предосторожности.

- Предоставьте пользователям возможность дать согласие на сбор данных до того, как вы начнете их собирать и куда-либо отправлять (в том числе сведения о сторонних аккаунтах, адресе электронной почты, номере телефона, установленных приложениях, файлах, сведения о местоположении и любые другие личные и конфиденциальные данные, о сборе которых пользователь может не знать).
- Обрабатывать все личные и конфиденциальные данные пользователя необходимо безопасным образом, в том числе с применением современных методов шифрования, например протокола HTTPS.
- Программное обеспечение, в том числе для мобильных устройств, должно передавать на сервер только те личные и конфиденциальные данные, которые необходимы для выполнения функций приложения.

Примеры нарушений:

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

Примеры правил в отношении пользовательских данных:

- *Правила Google Play в отношении пользовательских данных*
- *Правила в отношении пользовательских данных в рамках требований GMS*
- *Правила API Google в отношении пользовательских данных*

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.

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:

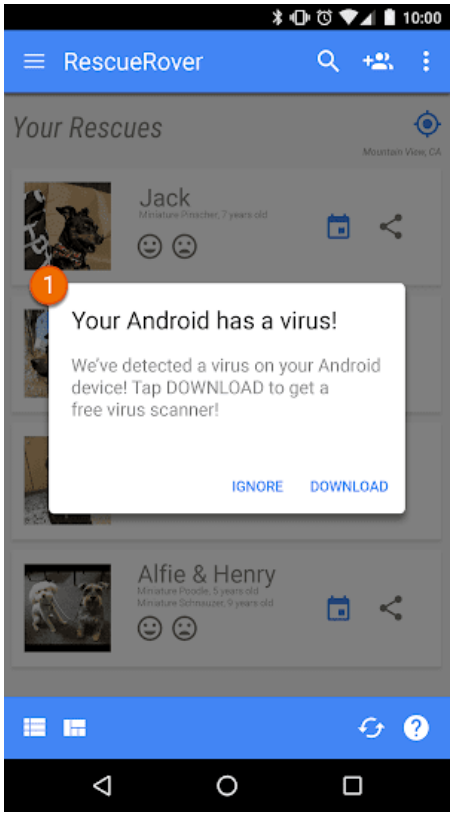
- Приложение, показывающее рекламу, которая не видна пользователям.
- Приложение, которое автоматически провоцирует нажатие на объявления без ведома пользователя или искусственно генерирует эквивалентный сетевой трафик для получения кликов.
- Приложение, отправляющее фальшивые ссылки на установку, чтобы 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.

Выдача себя за другое лицо

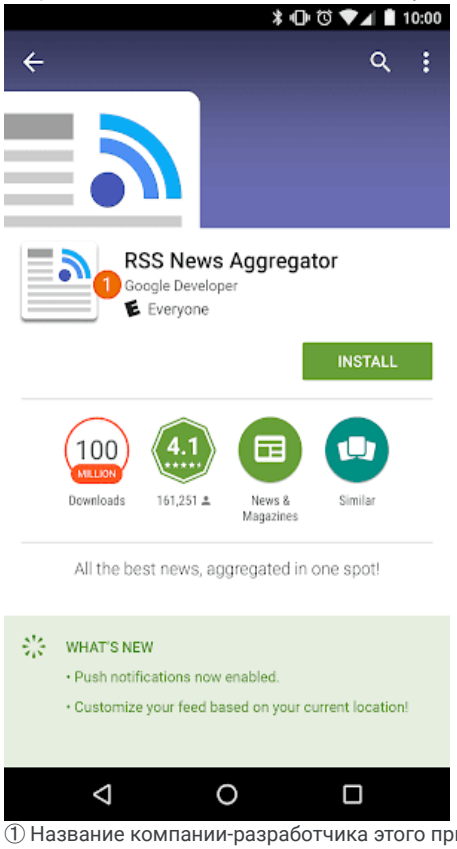
Когда разработчик выдает себя за другое лицо, это вредит и клиентам, и всему сообществу разработчиков. Запрещено публиковать приложения, которые вводят пользователя в заблуждение путем выдачи автора за другое лицо.

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.

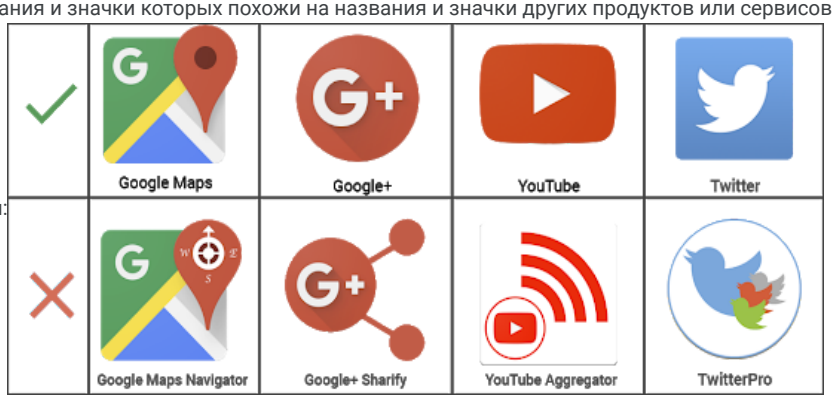
Вот примеры наиболее распространенных нарушений:

- 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.

- Приложения, названия и значки которых похожи на названия и значки других продуктов или сервисов до степени смешения:



Монетизация и реклама

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

Платежи

Платные приложения и приложения, в которых можно делать покупки, должны соответствовать перечисленным здесь требованиям.

Требования для платных приложений. Разработчики, которые взимают средства за приложения и их скачивание, должны использовать платежную систему Google Play.

Требования для приложений, в которых можно делать покупки:

- Для продажи цифровых товаров в играх, скачанных из Google Play, должна использоваться система оплаты контента через Google Play.
- Для продажи цифровых товаров в других категориях приложений, скачанных из Google Play, также должна использоваться система оплаты контента через Google Play. Исключения:

  - продажа физических товаров;
  - продажа цифрового контента, который можно использовать вне приложения (например, треков, которые можно воспроизводить в других проигрывателях).
- Виртуальная валюта должна использоваться только в том продукте, в котором она была куплена.
- Разработчикам запрещается вводить пользователей в заблуждение относительно приложений, а также услуг, товаров, контента и функций, которые можно в них приобрести. Если за доступ к функциям, указанным в описании приложения в Google Play, взимается плата, вы обязаны предупредить об этом пользователей.
- Если при покупках в приложении можно получить случайные виртуальные предметы (т. н. лутбоксы), вы должны явно сообщить пользователю о вероятности получения предметов до того, как он купит контент.

Ниже перечислены виды товаров, которые можно продавать, используя систему оплаты контента через Google Play.

- **Цифровой контент в играх.** Например, монеты, драгоценные камни, дополнительные жизни и ходы, а также специальные предметы, снаряжение, персонажи, аватары, дополнительные уровни и игровое время.
- **Функции и контент.** Например, возможность просматривать приложение без рекламы или возможности, недоступные в бесплатной версии.
- **Услуги, предоставляемые по подписке.** Например, передача музыки, видео, книг и т. д., а также цифровые публикации (в том числе в комплекте с бумажными версиями) и социальные сети.
- **Облачные программные продукты.** Например, хранилища данных, а также ПО для бизнеса и управления финансами.

Ниже перечислены виды товаров и услуг, для которых система оплаты контента через Google Play не поддерживается.

- **Розничные товары.** Например, продукты, одежда, товары для дома и электронные устройства.
- **Платные услуги.** Например, перевозка пассажиров и грузов, клининг, доставка еды, авиабилеты, билеты на мероприятия.
- **Членство (разовое и возобновляемое).** Например, в спортивных клубах, а также в клубах, предлагающих аксессуары, одежду или другие аналогичные товары. Сюда же относится участие в программах лояльности.
- **Разовое перечисление средств.** Например, перевод средств другому пользователю, онлайн-аукционы и пожертвования.
- **Онлайн-платежи.** Например, оплата задолженности по кредиту или счетов за коммунальные и телекоммуникационные услуги.

Обратите внимание, что для продажи физических товаров и услуг в приложениях можно использовать Google Pay API. Подробная информация приведена на странице Google Pay для разработчиков.

Подписки

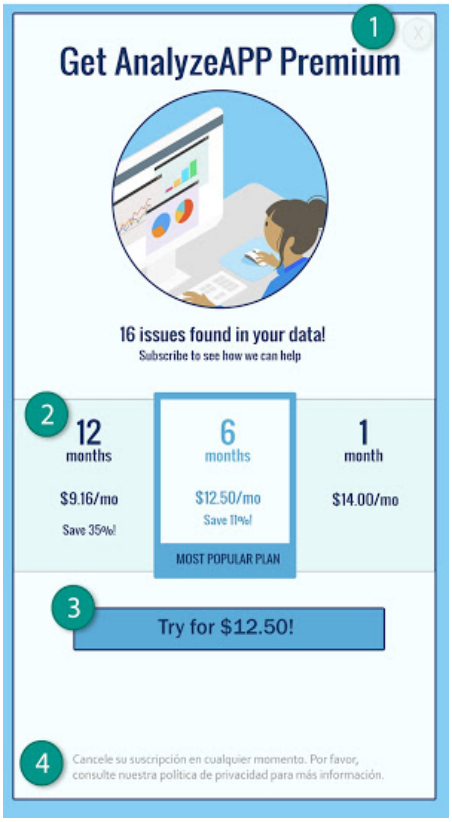
Разработчикам запрещается вводить пользователей в заблуждение относительно подписок или контента, который предлагается в приложениях. Ваше предложение должно быть сформулировано четко и ясно. Это относится к его размещению как на заставках, так и в самом приложении.

В приложении вы должно четко изложить свое предложение. Среди прочего необходимо ясно указать условия предложения, стоимость подписки и периодичность платежного цикла, а также уточнить, необходима ли подписка для работы с приложением. При этом все сведения должны быть указаны полностью, чтобы для ознакомления с информацией пользователю не требовалось выполнять дополнительные действия.

Вот примеры наиболее распространенных нарушений:

- Ежемесячные подписки, в условиях которых не указано, что они будут продляться автоматически каждый месяц со списанием средств со счета.
- Годовые подписки, где ярко выделена только 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: для подписки с автоматическим списанием средств дана
- формулировка "Бесплатная пробная версия".



① Кнопка "Закрыть" видна нечетко, и пользователь может не понять, что контент доступен и без подписки.

② В предложении указана цена только за один месяц, и 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 акции.

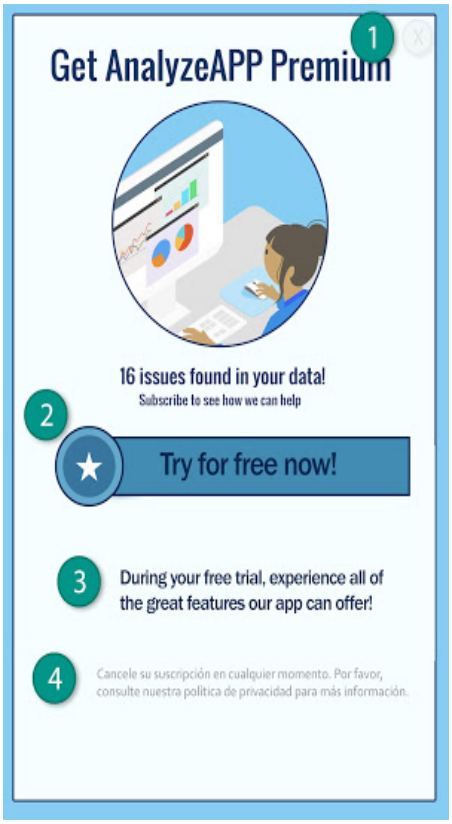
④ Информация в предложении и условиях использования представлена на разных языках, и пользователь может понять ее не полностью.

Бесплатные пробные версии и предложения для новых пользователей

Ещё до того, как пользователь приобретет подписку, вы должны ясно и точно сообщить ему условия предложения, включая его продолжительность и цену, а также описание доступного контента или сервисов. Не забудьте указать, как и когда пользователь перейдет с бесплатной пробной версии на платную подписку, уточнить стоимость платной подписки, а также сообщить, что подписку можно отменить до окончания бесплатного 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" видна нечетко, и пользователь может не понять, что контент доступен и без активации бесплатной пробной версии.

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, какой будет продолжительность бесплатного доступа к контенту.

④ Информация в предложении и условиях использования представлена на разных языках, и пользователь может понять ее не полностью.

Управление подписками и их отмена

Разработчик обязан явно сообщить пользователю, как изменить или отменить подписку в приложении.

Убедитесь, что правила подписки, ее отмены и возврата платежей не противоречат действующему законодательству, а также обязательно сообщайте пользователям обо всех изменениях в этих правилах.

Реклама

Запрещено публиковать приложения, содержащие рекламу, которая вводит в заблуждение или прерывает работу приложения. Объявления должны появляться только внутри приложения, быть приемлемыми для его целевой аудитории, а также соответствовать всем нашим правилам. Подробнее о правилах рекламы азартных игр...

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.

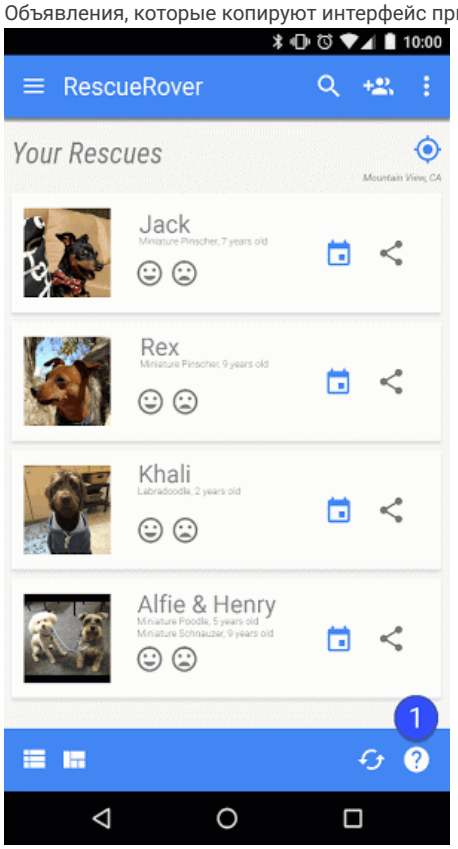
- Разрешения на доступ к данным о местоположении могут запрашиваться только для работы функций и сервисов, которые есть в приложении. Нельзя запрашивать доступ к данным о местоположении, если он будет использоваться только для рекламы.

Объявления, вводящие в заблуждение

Рекламные объявления не должны копировать интерфейс какого-либо приложения, системного уведомления или предупреждения. Пользователю должно быть понятно, к какому приложению относятся те или иные объявления.

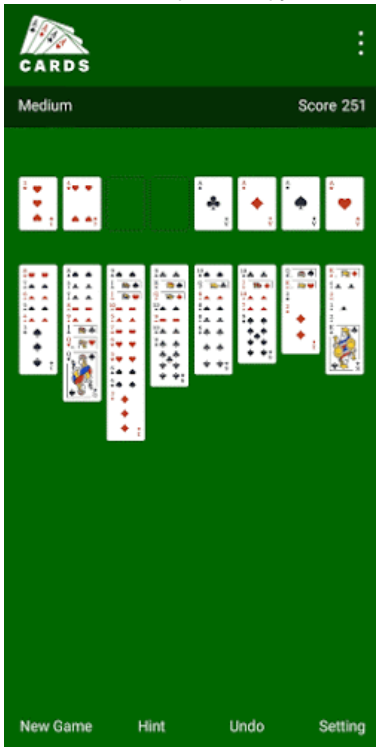
Вот примеры наиболее распространенных нарушений:

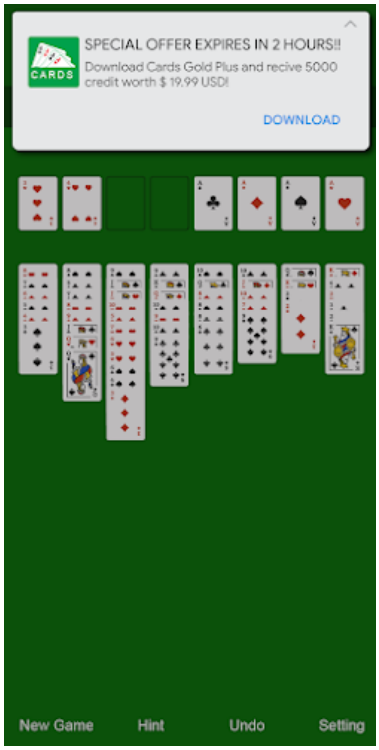
- Объявления, которые копируют интерфейс приложения:



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

- Объявления, которые копируют системные уведомления:



- 

Выше показаны примеры объявлений, которые внешне очень похожи на различные уведомления операционной системы.

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.

Объявления, прерывающие работу приложения

К этой категории относятся объявления, которые появляются в неожиданных местах, могут приводить к непреднамеренным нажатиям и нарушать функциональность устройства.

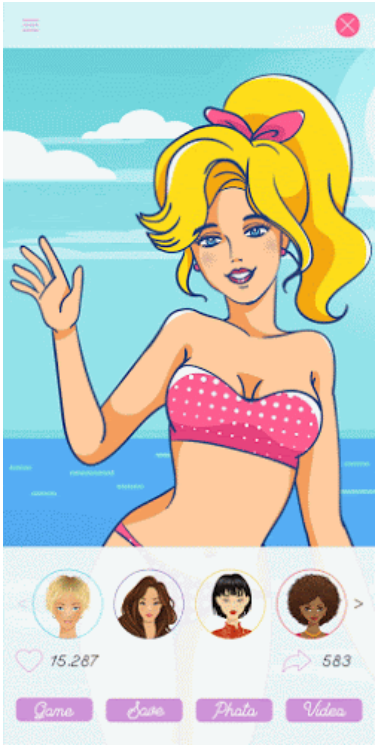
Запрещается вынуждать пользователя нажимать на объявление или отправлять личные данные для получения полного доступа к приложению. Межстраничные объявления могут отображаться только внутри приложения. Если в приложении есть межстраничные или другие объявления, которые прерывают обычный процесс использования, они должны легко закрываться.

Вот примеры наиболее распространенных нарушений:

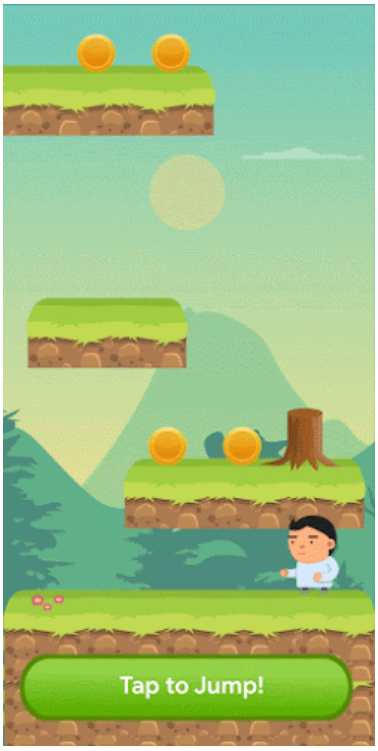
- Объявления, которые занимают весь экран, мешают работе с приложением и которые сложно закрыть:

① У этого объявления нет кнопки "Закрыть".

- Объявления, которые заставляют пользователя переходить по ссылкам с помощью ложной кнопки "Закрыть" или внезапного появления рекламы там, где расположены элементы управления, на которые пользователь обычно нажимает.



Объявление с ложной кнопкой "Закрыть".



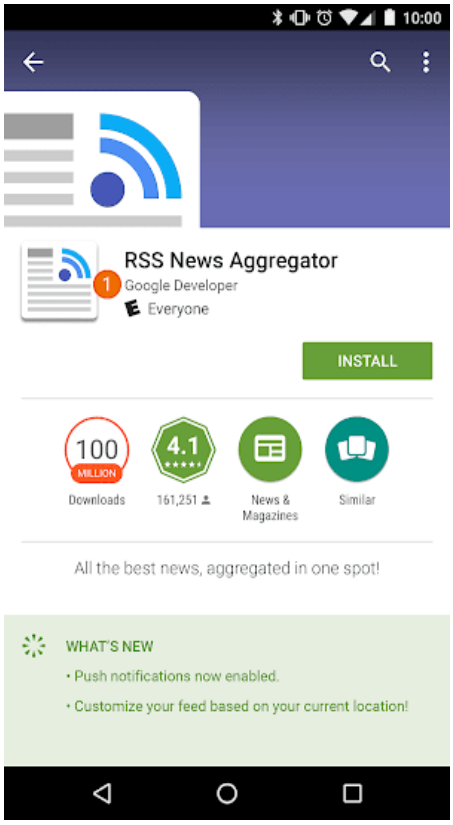
Объявление, которое внезапно появляется в той части экрана, на которую пользователь привык нажимать для доступа к функциям приложения.

Взаимодействие с приложениями, рекламой других разработчиков и функциями устройства

Объявления в вашем приложении не должны влиять на приложения других разработчиков 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. Объявления должны появляться только внутри приложения.

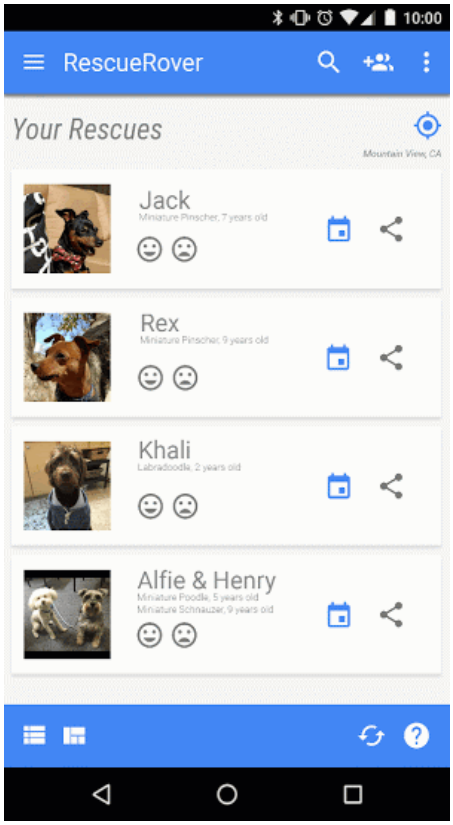
Вот примеры наиболее распространенных нарушений:

- Объявления, появляющиеся вне приложения:



Пользователь переходит из этого приложения на главный экран, и на нем внезапно появляется объявление.

- Объявления, которые возникают после нажатия кнопки главного экрана или выполнения других действий, предназначенных для выхода из приложения:

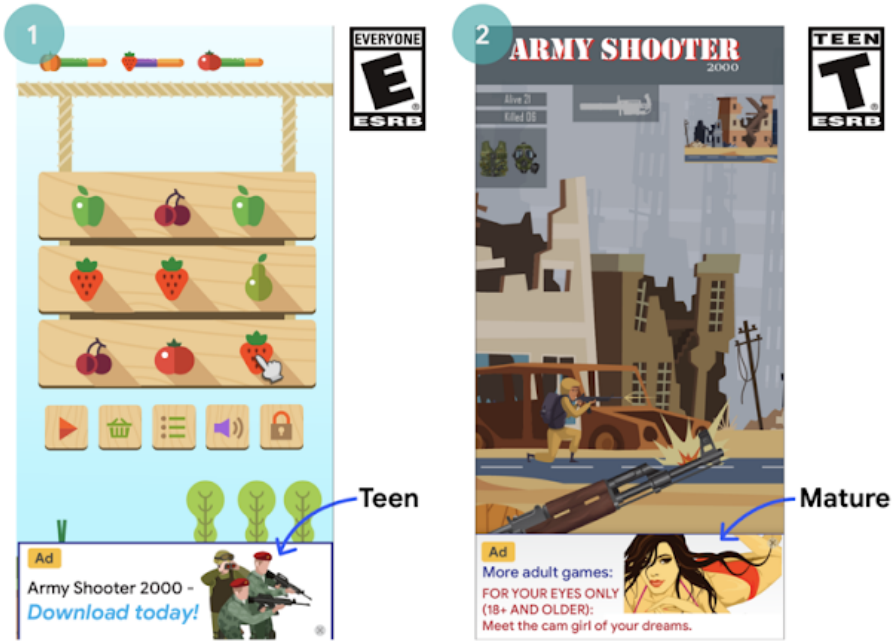


Пользователь пытается выйти из приложения на главный экран, и этот процесс прерывается показом объявления.

Неприемлемые объявления

Не только сам контент приложения должен соответствовать нашим правилам. Объявления в приложении должны быть приемлемы для его целевой аудитории.

Вот примеры наиболее распространенных нарушений:



① Объявление неприемлемо для целевой аудитории приложения (7+), поскольку предназначено для подростков.
② Объявление неприемлемо для целевой аудитории приложения (12+), поскольку предназначено для взрослых.

Использование рекламного идентификатора Android

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

- **Использование.** Рекламный идентификатор Android должен использоваться только для размещения рекламы и анализа ее показателей. При каждом обращении к идентификатору должны проверяться значения параметров "Отключить подбор рекламы" и "Отключить персонализацию 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 условии явно выраженного согласия пользователя.
  - Использование в аналитических целях. Рекламный идентификатор нельзя связывать с данными, позволяющими идентифицировать личность, или постоянными идентификаторами устройства, такими как SSAID, MAC-адрес или IMEI-код, без явно выраженного согласия пользователя.
- **Уважение предпочтений пользователя.** Новый идентификатор, присвоенный после сброса, нельзя связывать с предыдущим или его данными без явно выраженного согласия пользователя. Кроме того, нужно учитывать предпочтения 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. При этом разрешается контекстная реклама, ограничение частоты показов, отслеживание конверсий, создание отчетов, а также обнаружение угроз безопасности и случаев мошенничества.
- **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 настоящими правилами, причем это условие распространяется на всех, кому вы можете предоставить

идентификатор в ходе коммерческой деятельности. Во всех приложениях, загружаемых или публикуемых в Google Play, следует использовать рекламный идентификатор (если он доступен на устройстве). Применять для рекламных целей другие идентификаторы устройств запрещено.

Программа рекламы в приложениях для всей семьи

При размещении рекламы в приложении, предназначенном только для детей (как описано в правилах программы Приложения для всей семьи), необходимо использовать рекламные SDK, которые прошли самостоятельную сертификацию и подтвердили соответствие правилам Google Play, включая приведенные ниже требования к сертификации рекламных SDK. Если приложение рассчитано как на детей, так и на взрослых, вы должны предусмотреть проверку возраста пользователя и убедиться, что дети будут видеть объявления только из рекламных SDK с самостоятельной сертификацией. В приложениях, участвующих в программе "Приложения для всей семьи", запрещается использовать другие рекламные SDK.

Использование сертифицированных рекламных SDK становится обязательным только в том случае, если вы в целом применяете SDK для показа рекламы детям. Вы несете ответственность за контент объявлений и сбор сведений согласно правилам в отношении пользовательских данных и правилам программы "Приложения для всей семьи". При соблюдении этих условий мы не требуем сертификацию:

- 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 ресурсами.

Требования к сертификации рекламных SDK

- Определите признаки нежелательных объявлений и запретите их в условиях или политике рекламного SDK. Определения должны соответствовать Правилам программы Google Play для разработчиков.
- 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 действующие законы и постановления, например Закон США о защите личных сведений детей в Интернете (COPPA) и Генеральный регламент ЕС о защите персональных данных (GDPR). Кроме того, в ресурсах для детей в Google Play необходимо отключить в рекламных SDK персонализированную рекламу, рекламу на основе интересов, а также ремаркетинг.
- Разрешите издателям выбирать форматы объявлений, соответствующие правилам в отношении рекламы и монетизации программы "Приложения для всей семьи", а также программы "Одобрено преподавателями".
- Если для показа рекламы детям используется технология назначения ставок в реальном времени, убедитесь, что файлы объявления проверены, а участникам аукциона передаются индикаторы конфиденциальности.
- Предоставьте Google информацию, указанную в заявке и необходимую для проверки рекламного SDK на соответствие всем требованиям, и своевременно отвечайте на последующие запросы информации.

Примечание. Необходимо использовать рекламные SDK для показа объявлений в соответствии со всеми законами и положениями относительно детей, применимыми к деятельности издателей.

Требования к платформам-посредникам, которые показывают рекламу детям:

- Вы должны использовать только рекламные SDK, сертифицированные Google Play, или принимать меры предосторожности, гарантирующие, что все объявления на платформах-посредниках соответствуют этим требованиям.
- Необходимо передавать информацию о рейтинге рекламного контента и о том, что ресурс предназначен для детей.

Список сертифицированных рекламных SDK опубликован здесь.

Если вы знаете организации, которые хотят сертифицировать свои рекламные SDK, то можете отправить им ссылку на эту форму.

Данные для Google Play и продвижение

Методы, которые вы применяете для продвижения своего приложения, значительно влияют на восприятие Google Play посетителями. Не используйте спам и рекламу низкого качества, 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 либо сообществу разработчиков. Сюда относятся приложения, выполняющие перечисленные ниже действия.

- Использование объявлений, вводящих в заблуждение, на веб-сайтах, в приложениях и других объектах, включая копирование уведомлений операционной системы.
- Распространение и установка, в результате которых происходит направление пользователей в Google Play или скачивание приложения без предварительного запроса.
- Нежелательное рекламирование через SMS.

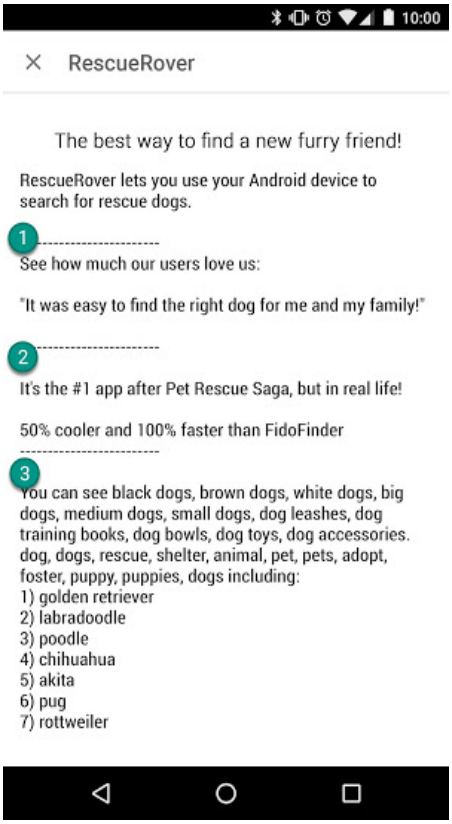
Вы обязаны следить за тем, чтобы в рекламных сетях и партнерских программах соблюдались эти правила и не использовались запрещенные методы продвижения.

Метаданные

Мы запрещаем публиковать приложения с ложными, неправильно отформатированными, недостаточными, нерелевантными, излишними или недопустимыми метаданными. К метаданным, помимо всего 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.

Кроме того, в соответствии с правилами 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.

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

- Изображения и видео сексуального характера. Не используйте материалы, содержащие изображения женской груди, ягодиц, гениталий и других откровенных изображений человеческого тела, будь то рисунки или фотографии.

- Непристойная лексика и другие речевые конструкции, недопустимые для широкой аудитории, в описании приложения в Google Play.
- Изображение сцен насилия на значках приложения, в рекламных изображениях и видеороликах.
- Изображение нелегального употребления наркотиков, даже если это образовательный, документальный, научный или художественный контент. Данные на странице приложения должны подходить для любой аудитории.

Вот некоторые советы по продвижению вашего приложения:

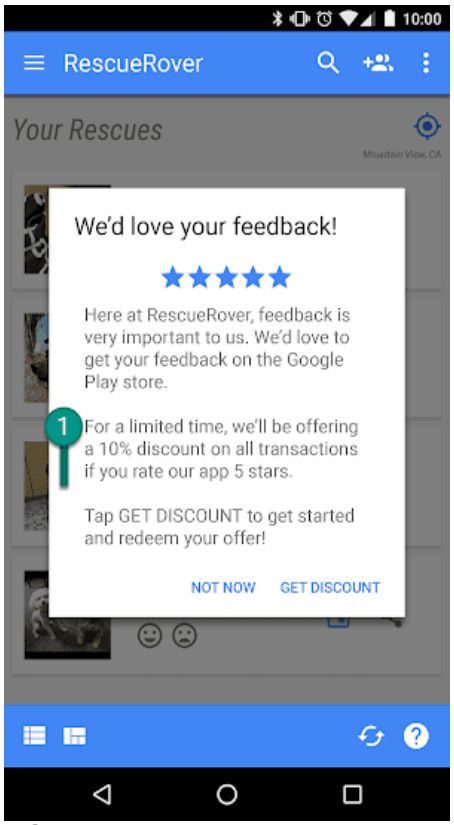
- Расскажите, почему ваше приложение особенное, что выделяет его среди остальных и чем оно может понравиться пользователям.
- Убедитесь, что название и описание дают точное представление о приложении и его функциях.
- Не используйте повторяющиеся или не связанные с приложением ключевые слова и ссылки.
- Следите за тем, чтобы описание приложения было емким и понятным. Помните: короткие описания легче читать, особенно на устройствах с небольшим экраном. Слишком большой объем и плохое форматирование текста, а также излишние подробности и повторы могут стать причиной несоответствия правилам.
- Не забывайте, что страница вашего приложения должна подходить для широкой аудитории. Не используйте в данных для Google Play запрещенные изображения, видеоматериалы или текст.

Оценки, отзывы и количество установок

Разработчикам запрещено предпринимать попытки изменить позицию какого-либо приложения в рейтинге Google Play, например с помощью мошеннических установок, оплаченных или ложных оценок и отзывов.

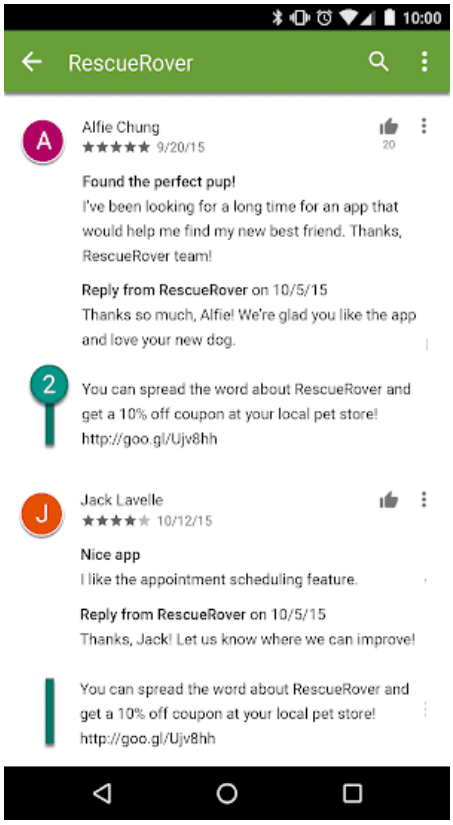
Вот примеры наиболее распространенных нарушений:

- Просьбы оценить приложение в обмен на поощрение:



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

- Многократное выставление оценок с целью повлиять на позицию приложения в рейтинге Google Play.
- Публикация отзывов, содержащих недопустимые сведения (включая информацию о партнерах, купонах, игровых кодах, адреса электронной почты или ссылки на веб-сайты либо другие приложения), а также поощрение пользователей делать это:



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

Оценки и отзывы служат контрольными показателями качества приложения, поэтому они должны быть честными и не должны отклоняться от темы. Вот несколько советов о том, как отвечать на отзывы пользователей:

- Не уклоняйтесь от обсуждения упомянутых проблем и не просите повысить оценку.
- Посоветуйте справочные ресурсы, например укажите адрес службы поддержки или страницы с часто задаваемыми вопросами.

Возрастные ограничения

Система возрастных ограничений в Google Play создана для того, чтобы разработчики могли сообщать пользователям, для какой аудитории подходят приложения в их стране. Она включает официальные категории Международной коалиции возрастной классификации (IARC). Представительства IARC в отдельных странах при определении возрастной категории контента в приложении следуют соответствующим рекомендациям. Запрещена публикация приложений без указаний возрастных ограничений.

Зачем 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 узнать, к какой возрастной категории относятся ваши приложения и игры, необходимо заполнить анкету в Play Console, описав 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 важно предоставить как можно более точную информацию.

Заполнить анкету нужно для каждого приложения независимо от даты публикации, иначе ему будет присвоен статус "Без классификации".

Если вы вносите в контент или функции приложения изменения, которые влияют на ответы в анкете, вы должны заполнить ее ещё раз.

Чтобы узнать больше об организациях по оценке контента и о том, как заполнить анкету, перейдите в Справочный центр.

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

Запрещено размещать в категории "Новости" приложения, которые заявлены как новостные, но при этом не публикуют соответствующий контент. Новостные приложения, которые требуют приобретения подписки, должны перед покупкой предоставлять часть контента в режиме предварительного просмотра.

Новостные приложения ДОЛЖНЫ:

- содержать достоверную информацию об издателе новостей и их источниках, в том числе данные о владельце;
- иметь сайт или страницу в приложении, где указаны актуальные контактные данные издателя новостей.

Новостные приложения НЕ ДОЛЖНЫ:

- содержать материалы с явными грамматическими и орфографическими ошибками;
- содержать исключительно статический контент;
- иметь в качестве основной цели получение дохода от рекламы или занятие партнерским маркетингом.

Новостные агрегаторы должны явно указывать источник контента в приложении. Каждый из этих источников должен соответствовать правилам в отношении новостей.

Спам и функциональность

Приложения должны содержать хотя бы минимальный набор функций и работать корректно. Если в приложении постоянно происходят сбои, а также если оно бесполезно или создано для распространения спама среди пользователей либо в Google Play, то такое приложение не имеет никакой ценности.

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.

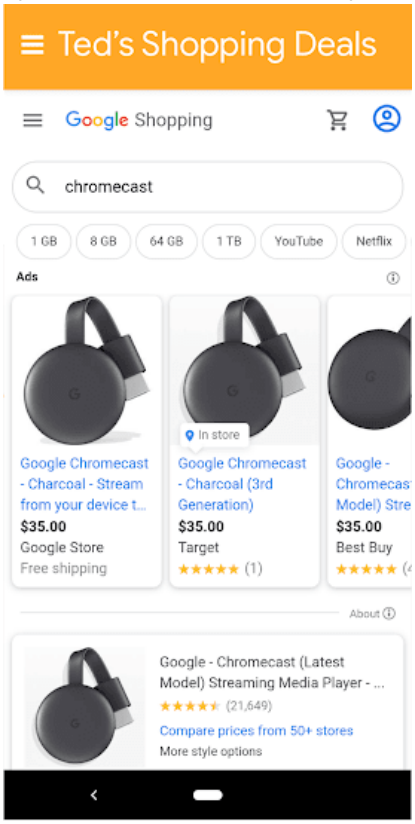
Спам с целью перенаправления трафика

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:



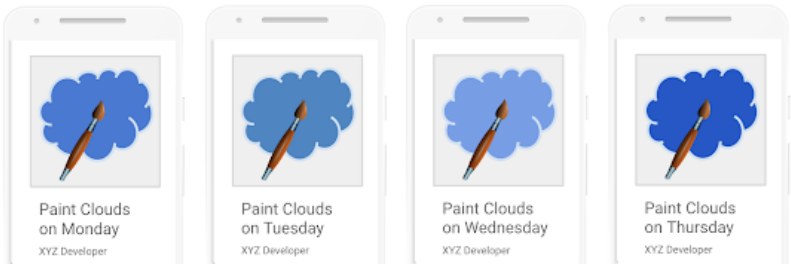
Это приложение называется "Выгодные товары у Теда" и просто перенаправляет пользователей в Google Покупки.

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.



Рекламные приложения

Запрещается публиковать приложения, основной целью которых является показ рекламы.

Вот примеры наиболее распространенных нарушений:

- Приложения, в которых межстраничные объявления демонстрируются после каждого действия пользователя, включая клики, пролистывания и т. д.

Функциональность

Убедитесь, что ваше приложение работает стабильно и корректно, а также представляет ценность для пользователей.

Вот примеры наиболее распространенных нарушений:

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

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 с мгновенным запуском

Приложения с мгновенным запуском должны быть удобными в использовании, а также соответствовать высоким 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 требования

При разработке приложений для Android 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

Приложение с мгновенным запуском не должно вносить в устройство пользователя изменения, которые сохраняются дольше, чем сеанс работы этого приложения. Например, оно не должно менять обои или создавать виджет на главном экране.

Видимость работы приложения

Работа приложения с мгновенным запуском не должна быть скрыта от пользователя.

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. Примеры подобных идентификаторов:

- 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 идентифицировать 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.

Приложения для всей 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.

Разработка приложений для детей и 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.

Приложения, разработанные специально для детей, должны быть включены в программу "Приложения для всей семьи". Подать заявку на участие в ней также можно в случае, если дети входят в целевую аудиторию. Все приложения, предназначенные для всей семьи, потенциально смогут участвовать в программе "Одобрено преподавателями", но мы не можем гарантировать, что они точно будут в нее включены. Даже если вы не захотите включать свой контент в программу "Приложения для всей семьи", вам нужно будет соблюдать приведенные ниже требования, а также другие Правила программы для разработчиков и условия Соглашения о распространении программных продуктов.

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 термины, которые можно посчитать ориентированными на детей. Команда Google Play оставляет за собой право проверять предоставленную информацию о приложении и определять, точно ли выбрана целевая аудитория.

Если вы укажете, что приложение предназначено только для взрослых, но Google придет к другому выводу, вы сможете добавить для пользователей ярлык с предупреждением.

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

1. **Контент приложения.** Контент, доступный детям, должен подходить для них.
2. **Ответы на вопросы в Google Play Console.** Вы должны точно отвечать в Google Play Console на все вопросы о своем приложении и обновлять ответы, когда вносите в него изменения.
3. **Реклама.** Если вы показываете в приложении рекламу для детей или пользователей, чей возраст неизвестен, то должны:
   - использовать для показа объявлений таким пользователям только рекламные SDK, сертифицированные Google Play;
   - исключить для таких пользователей ремаркетинг (рекламу, направленную на определенных пользователей и зависящую от истории взаимодействия с сайтом или приложением) и рекламу на основе интересов (рекламу, направленную на отдельных пользователей, чье поведение в сети 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.
4. **Сбор данных.** Если ваше приложение собирает какую-либо личную или конфиденциальную информацию детей, в том числе с помощью API и SDK, вы должны сообщить об этом в явной форме. К конфиденциальной информации относятся, например, учетные данные, данные с микрофона и камеры, данные об устройстве, идентификатор Android, данные об использовании объявлений и рекламный идентификатор.
5. **API и SDK.** Убедитесь, что API и SDK используются в вашем приложении надлежащим образом.
   - Приложения, единственной целевой аудиторией которых являются дети, не должны использовать API или SDK, которые не одобрены для рассчитанных на детей сервисов. Это относится в том числе к входу с аккаунтом Google (и другим API Google, которые имеют доступ к данным аккаунта), игровым сервисам Google Play и любым API, которые используют для аутентификации и авторизации технологию OAuth.
   - В приложениях, предназначенных как для детей, так и для взрослых, нельзя использовать API или SDK, которые не одобрены для рассчитанных на детей сервисов. Исключения возможны, если API или SDK применяются только после проверки с помощью нейтрального возрастного фильтра или если при их использовании данные детей не собираются (например, когда вход с аккаунтом Google является дополнительной функцией). Приложения, предназначенные как для детей, так и для взрослых, не должны подразумевать использование API или SDK, которые не одобрены для рассчитанных на детей сервисов, для входа или получения доступа к контенту.
6. **Политика конфиденциальности.** На страницу приложения в Google Play необходимо добавить ссылку на свою политику конфиденциальности. Ссылка должна работать все время, пока приложение доступно в Google Play. Политика конфиденциальности, помимо прочего, должна содержать точную информацию о том, как именно ваше приложение собирает и использует данные.
7. **Особые ограничения:**
   - Если приложение использует дополненную реальность, при ее запуске 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").
  - Приложение не должно требовать использования устройств, не рекомендованных для детей (например, Daydream или Oculus).

8. **Соблюдение законодательства.** Ваше приложение, как и все выполняемые или используемые им API и SDK, не должно 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). Информацию о правилах Google Play относительно рекламы, покупок в приложении и коммерческого контента, предназначенного для детей, можно найти на этой странице.

Программа "Приложения для всей семьи"

Приложения, разработанные специально для детей, должны быть включены в программу "Приложения для всей семьи". Если ваше приложение предназначено для всех аудиторий, в том числе для детей и семейного просмотра, вы тоже можете подать заявку на участие в этой программе.

Перед подачей заявки убедитесь, что приложение соответствует требованиям программы "Приложения для всей семьи" и критериям допуска в нее, а также Правилам программы для разработчиков и условиям Соглашения о распространении программных продуктов.

Подробнее о том, как подать заявку на участие в программе…

Проверка на соответствие требованиям программы

Контент и реклама во всех приложениях, участвующих в программе "Приложения для всей семьи", должны быть рассчитаны на детей и соответствовать приведенным ниже правилам. Эти требования должны соблюдаться все время, пока приложение участвует в программе. Команда Google Play оставляет за собой право отклонять, удалять и блокировать приложения, не соответствующие правилам.

Требования программы "Приложения для всей семьи"

1. Приложение должно иметь возрастное ограничение "Для всех" или "10+" (по классификации ESRB) или аналогичное им.
2. При заполнении анкеты для присвоения возрастного ограничения в Google Play Console вы должны сообщить точную информацию обо всех интерактивных элементах приложения, в том числе указать:
   - могут ли пользователи взаимодействовать друг с другом или обмениваться информацией;
   - передает ли приложение личные данные пользователей третьим лицам;
   - передает ли приложение информацию о местоположении пользователя другим людям.
3. Если ваше приложение использует Android Speech API, значение параметра RecognizerIntent.EXTRA_CALLING_PACKAGE должно соответствовать названию пакета приложения (PackageName).
4. В приложениях должны использоваться только рекламные SDK, сертифицированные Google Play.
5. Приложения, созданные специально для детей, не могут запрашивать доступ к данным о местоположении.
6. Для запроса подключения по Bluetooth необходимо использовать класс CompanionDeviceManager. Это правило не распространяется на приложения, предназначенные исключительно для версий ОС, которые не поддерживают этот класс.

Вот примеры приложений, которые не подходят для участия в программе:

- Приложения с рейтингом "Для всех", рекламирующие азартные игры.
- Приложения для родителей или опекунов (например, руководство по воспитанию детей или приложение для отслеживания грудного вскармливания).
- Руководства для родителей или приложения для управления устройствами, предназначенные только для родителей или опекунов.
- Приложения, значок которых недопустим для детей.

Категории

Если вашу заявку на участие в программе одобрят, вы сможете выбрать для приложения ещё одну категорию, которая описывает его наилучшим образом.

Приключения. Экшен-игры, в том числе гонки, сказочные квесты и другие приложения, вызывающие эмоциональный подъем.

Игры для ума. Различные головоломки, в том числе пазлы, игры для поиска одинаковых картинок, тесты и другие приложения, развивающие память, интеллект или логику.

Творчество. Игры и приложения, которые стимулируют творчество, например приложения для рисования и обучения программированию.

Образование. Игры и приложения, разработанные при участии преподавателей или других экспертов в области образования и способствующие обучению (в том числе формированию базовых жизненных навыков и критического мышления), а также социально-эмоциональному, физическому и творческому развитию.

Музыка и видео. Игры и приложения с музыкой или видео, например виртуальные синтезаторы, а также видео- и аудиопроигрыватели.

Ролевые игры. Приложения, в которых ребенок играет какую-то роль, например доктора, повара, принцессы, пожарного, полицейского или вымышленного героя.

Реклама и монетизация

Реклама в приложениях, участвующих в программе "Приложения для всей семьи" или подпадающих под требования к приложениям для детей, должна соответствовать перечисленным ниже правилам. Они относятся к любой рекламе ваших и сторонних приложений, 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, слишком настойчиво предлагающих платный контент.

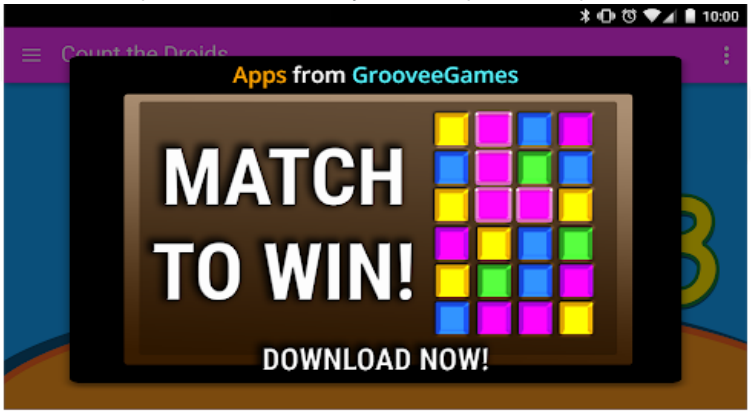
Требования к формату объявлений

Рекламные объявления и предложения сделать покупку в приложении не должны использовать контент, вводящий в заблуждение, и не должны быть предназначены для того, чтобы провоцировать ребенка на необдуманные нажатия. Запрещены следующие приемы:

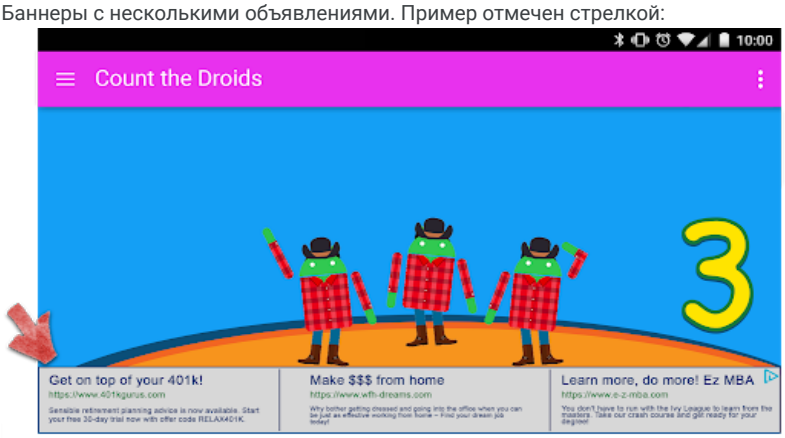
- Объявления, прерывающие работу приложения, в том числе занимающие весь экран или мешающие работе с приложением, которые сложно закрыть (например, полноэкранные объявления).
- Объявления, которые мешают нормальной работе приложения или игры и не закрываются через 5 секунд. Объявления, которые не мешают нормальной работе приложения или игры, могут не закрываться через 5 секунд (например, видеоклип со встроенной рекламой).
- Межстраничные объявления или предложения совершить покупку, которые появляются сразу после запуска приложения.
- Размещение нескольких объявлений на странице. Например, одновременный показ более одного баннера или видеообъявления, рекламные баннеры, которые содержат несколько предложений в одном месте размещения.
- Объявления или предложения совершить покупку, которые сложно отличить от контента приложения.
- Использование шокового эффекта и тактик эмоционального манипулирования, чтобы провоцировать пользователей на просмотр объявлений или на покупку в приложении.
- Отсутствие четкого указания на различия между виртуальной валютой и реальными деньгами при покупках в приложении.

Вот примеры наиболее распространенных нарушений:

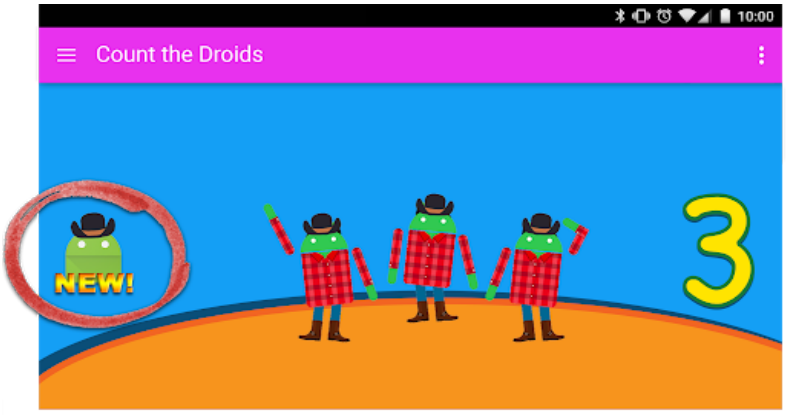
- Объявления, которые перемещаются по экрану, чтобы пользователь не мог их закрыть.
- Объявления, которые занимают большую часть экрана и которые непонятно, как закрыть. Например:



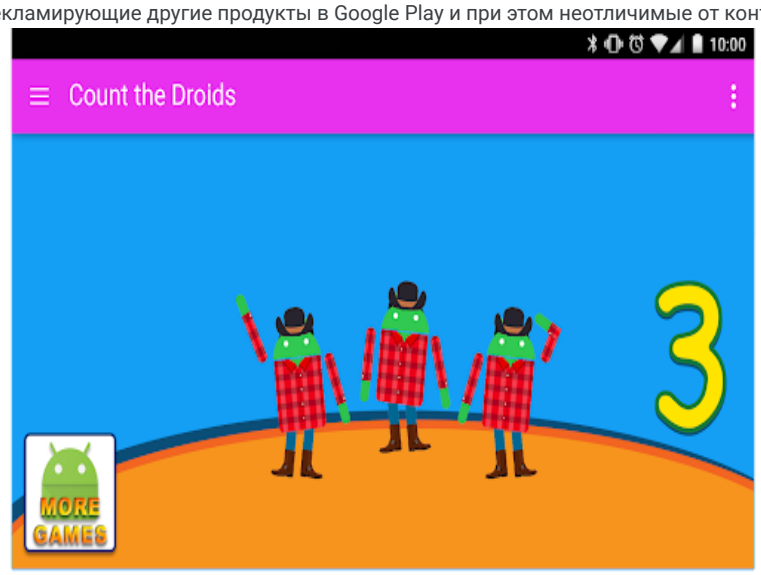
- Баннеры с несколькими объявлениями. Пример отмечен стрелкой:



- Объявления, которые можно принять за контент приложения. Пример:



- Кнопки или объявления, рекламирующие другие продукты в Google Play и при этом неотличимые от контента приложения. Например:



Детям нельзя показывать следующие объявления:

- **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.
- **Контент для взрослых и материалы сексуального характера.** Реклама с эротическим и сексуальным содержанием.
- **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 рекламные SDK, сертифицированные Google Play. 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 рекламные SDK, сертифицированные Google Play. В приложениях, участвующих в программе "Приложения для всей семьи", запрещается использовать другие рекламные SDK.

Подробные требования к объявлениям и список сертифицированных рекламных SDK можно найти на этой странице.

Если вы используете сервис "Реклама в приложении", 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.

Покупки в приложении

Перед покупкой в приложении, участвующем в программе "Приложения для всей семьи", пользователю нужно пройти повторную аутентификацию. Это гарантирует, что покупку совершает финансово ответственный человек, а не ребенок.

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. Сообщите нам, если обнаружите нарушение или у вас возникнут вопросы о нем.

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. Для таких приложений может проводиться дополнительная проверка на соблюдение правил.

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

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, 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

Если ваше приложение нарушает любые из наших правил, мы примем соответствующие меры. Мы предоставим вам информацию о своих действиях по электронной почте, а также сообщим, как подать апелляцию, если вы считаете, что мы ошиблись.

Обратите внимание, что удаление или предупреждение может касаться не всех нарушений, допущенных в вашем приложении или каталоге приложений. Разработчики обязаны сами устранять нарушения и проверять свой контент на соответствие нашим правилам. Невозможность устранения нарушений во всех приложениях может стать причиной дополнительных принудительных мер.

Повторные или серьезные нарушения этих правил (например, мошенничество или размещение вредоносного ПО) или нарушение Соглашения о распространении программных продуктов приведет к удалению аккаунтов разработчика.

Принудительные меры

В этом разделе представлены возможные действия со стороны Google Play и их потенциальные последствия для вашего приложения/аккаунта разработчика Google Play. Также эта информация разбирается в видео.

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 предложение заново, пока не устраните нарушения.

Удаление

- Приложение, а также все предыдущие его версии, будет удалено из Google Play. Пользователи больше не смогут его скачать.
- Пользователи не смогут просматривать описание приложения, число установок, статистику и оценки. Информация будет восстановлена, если вы загрузите версию, которая отвечает всем требованиям.
- 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 будет много, действие аккаунта может быть приостановлено.

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

Блокировка

- Приложение, а также все предыдущие его версии, будет удалено из Google Play. Пользователи больше не смогут его скачать.
- Серьезные и систематические нарушения правил, а также повторные отклонения и удаления приложения могут привести к его блокировке.
- Пользователи не смогут просматривать описание приложения, число установок, статистику и оценки. Информация будет восстановлена, если вы загрузите версию, которая отвечает всем требованиям.
- Вы больше не сможете использовать APK и набор App Bundle заблокированного приложения.
- Пользователи потеряют возможность делать покупки в приложении и использовать другие платежные функции, пока новая версия, отвечающая всем требованиям, не будет одобрена Google Play.
- Блокировка вредит репутации вашего аккаунта разработчика Google Play. Неоднократные блокировки могут привести к прекращению действия личного аккаунта, а также связанных с ним аккаунтов разработчика Google Play.

Примечание. Не пытайтесь повторно опубликовать заблокированное приложение без разрешения Google Play.

Ограничение видимости

- Видимость вашего приложения в Google Play будет ограничена. При этом оно по-прежнему будет 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 описание приложения, число установок, статистику и оценки.

Прекращение действия аккаунта

- Прекратив действие вашего аккаунта разработчика, мы удалим из Google Play все приложения в вашем каталоге и запретим вам публиковать новые. Все связанные аккаунты разработчика также будут заблокированы навсегда.

Связаться с нами

Расскажите о своей проблеме нашим сотрудникам

- Повторные или серьезные нарушения правил могут привести к прекращению действия вашего аккаунта Play Console.
- Поскольку приложения, опубликованные через этот аккаунт, будут удалены, пользователи не смогут просматривать страницы приложений, число установок, статистику и оценки.

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

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, следуя инструкциям, отправленным вам по электронной почте.

Дополнительные ресурсы

Если у вас есть вопросы о принудительных мерах в отношении вашего приложения или об оценке/комментарии пользователя, ознакомьтесь с приведенными ниже материалами или свяжитесь с нами через Справочный центр. Обратите внимание, что мы не можем обеспечить вам юридическую помощь, поэтому рекомендуем при необходимости обратиться к юристу.

- Проверка приложений и апелляции
- Как сообщить о нарушении правил
- Как обратиться в Google Play по поводу удаления приложения или блокировки аккаунта
- Предупреждения
- Как сообщить о недопустимых отзывах
- Мое приложение было удалено из Google Play
- Прекращение действия аккаунта разработчика Google Play