Декларация ЕС принципов саморегулирования
в целях безопасности в Интернете

Неофициальный перевод

1. **I. Об этих принципах**

Провайдеры социальных сетей (соцсетей), перечисленные в конце этого документа, преследуют общую цель – максимизировать пользу и преимущества от использования Интернета, регулируя потенциальные риски для детей и молодежи.Для их защиты отдельные компании разрабатывают и развивают стратегии безопасности.Многие провайдеры также принимают активное участие в межотраслевых мероприятиях и организациях в рамках ЕС, целью которых является обсуждение существующих на рынке позитивных практик.Примерами такого сотрудничества могут выступать *Специальная комиссия домашнего офиса Соединенного королевства по защите детей в Интернете*, документ *Основы прав человека для интернет-провайдеров*, разработанный Европейским советом совместно с Европейской ассоциацией интернет-провайдеров (EuroISPA) и такими образовательными проектами, как «*Учить сегодня»*.Подобные мероприятия и проекты также разрабатываются в странах за пределами ЕС.

Эти принципы были разработаны компаниями-провайдерами соцсетей при поддержке Европейской комиссии, а также ряда неправительственных организаций, как часть *Программы по обеспечению безопасного использования сети Интернет* для предоставления рекомендаций и описания существующих позитивных практик провайдерам социальных сетей и других пользовательских интерактивных сайтов с целью повышения уровня безопасности детей и молодежи при использовании онлайн сервисов. Провайдеры соцсетей часто работают с множеством территорий по всей Европе, одновременно в нескольких странах, и приветствуют возможность руководствоваться общеевропейскими принципами в этой области.

Документ кратко рассказывает о принципах, которыми компании-провайдеры соцсетей должны руководствоваться при реализации активностей по минимизации потенциального ущерба для детей и молодежи, а также описывает ряд удачных подходов и примеров, которые могут помочь в реализации этих принципов.Данное руководство не является решением на все случаи жизни.В нем признается, что интернет-индустрия очень разнообразна и включает в себя как глобальных игроков, так и небольшие локальные сервисы.Соцсети сильно разнятся по типу предлагаемых услуг, платформам, на которых они могут использоваться, по демографии пользователей, рынкам, на которых они работают, и юрисдикциям, на которых они основаны.Все эти факторы влияют на уровни и типы рисков, присущих этим сервисам, а также на стратегии, которые могут быть подходящими и целесообразными для реагирования на такие риски.

Соответственно, провайдеры, определяя собственные стратегии безопасности, используют эти принципы, учитывают индивидуальные особенности своих сервисов и применяют подходящие для них

рекомендации. Поэтому, в то время, как провайдеры поддерживают все семь перечисленных в документе принципов, каждый из них самостоятельно определяет, где и насколько четко применять определенные рекомендации документа.Эти принципы не являются обязательными для исполнения, однако их использование провайдерами настоятельно рекомендуется.

Одновременно с этими принципами в ЕС и других странах ведется ряд дискуссий, направленных на формирование устоявшейся и органичной системы взглядов и практик, на основе которой провайдеры могут создавать и разрабатывать стратегии защиты детей и молодежи.Применение провайдерами данных принципов, важность этого документа, а также актуальность представленных в нем примеров будут оценены, как показано ниже, в процессе консультаций с Европейской комиссией и другими заинтересованными сторонами.

Эти принципы призваны предоставить руководство для Сервисов Социальных Сетей, которыми могут пользоваться дети и подростки. В контексте этих принципов термин «Сервисы Социальных Сетей» относится к онлайн-сервисам, которые отвечают следующим свойствам:

- Платформа, которая обеспечивает социальное взаимодействие онлайн между двумя и более людьми с целью создания дружественных отношений, организации встреч с другими людьми или в целях обмена информацией;
- Ее функционал позволяет пользователям создавать и самостоятельно заполнять личные профили с такой информацией, как имя или псевдоним пользователя, фотографии, размещенные пользователем на персональной странице, другая персональная информация о пользователе, а также ссылки на другие персональные страницы, расположенные на сервисе, страницы друзей или связанные с пользователями, к которым могут получить доступ другие пользователи или посетители сервиса;
- Содержит механизмы такие связи с другими пользователями, как доски сообщений, электронная почта или системы мгновенного обмена сообщениями;
- Содержит инструменты, которые позволяют пользователям осуществлять поиск других пользователей в соответствии с информацией, которую пользователи указали в своем профиле и открыли ее для других пользователей.

Доступ к сервисам социальных сетей можно получить с помощью ряда платформ.Функционал отдельных платформ может разниться, и провайдер может не иметь возможности обеспечить доступность одинаковых функций на всех платформах.Сервисы также могут быть доступны в виде загружаемых приложений.На практике провайдеры будут работать в условиях ограничений этих платформ и каналов распространения информации, учитывая обозначенные в данном документе принципы.

В социальных сетях все больше используются интерфейсы программирования приложений (API), которые подчеркивают открытую, рассредоточенную и объединяющую природу Интернета. API позволяют

сторонним компаниям-разработчикам создавать «приложения», а в некоторых случаях пользователи могут добавить такие приложения в свои профили в соцсетях, что дает возможность расширять доступные им утилиты и функционал. Так как приложения являются новым и развивающимся свойством соцсетей, а природа взаимодействия между разработчиками приложений и компанией-провайдером соцсетей уникальна в каждом случае, соцсети могут предлагать различные уровни гарантий своим пользователям в рамках этих принципов. Эти уровни гарантий будут описаны в примечаниях к руководству в Приложении 1.

II. Предпосылки

Понятие потенциальных рисков для детей и подростков в социальных сетях

Интернет вместе с другими новыми технологиями за последние пятнадцать лет предоставил пользователям огромные преимущества и возможности в связи, информации, электронной коммерции и развлечениях. Последняя волна технологий, сгруппированных под названием «технологии web 2.0» и включающих в себя социальные сети, привели в действие дополнительную эволюцию в способах, с помощью которых люди, особенно молодежь, связываются с друзьями, получают доступ к развлечениям и общаются в сообществах по интересам.

Как и в случаях с многими другими продуктами и услугами, злоупотребление этими технологиями может содержать потенциальную опасность для детей и подростков.Компании-провайдеры соцсетей должны оценивать, насколько эти потенциальные риски применимы к их сервисам. Потенциальные онлайн-риски для детей и подростков можно разделить на четыре категории:

- Нелегальный контент, к примеру, изображения жестокого обращения с детьми и высказывания, пропагандирующие ксенофобию и нетерпимость;

- Контент, не предназначенный для просмотра лицами, не достигшими 18 лет. К примеру, порнография или материалы сексуального характера, насилие или другой контент для взрослых, который может быть неуместен для просмотра детьми и подростками;

- Контакты взрослых с детьми и подростками или детей и подростков друг с другом с целями сексуального характера;

- Такие типы поведения пользователей онлайн, как запугивание или издевательства (распространение слухов, исключение участников из чьей-либо социальной группы, а также удаление из группы друзей или ограничение доступности информации), поведение, которое может содержать потенциальный риск (к примеру, разглашение персональной информации, публикация сексуальных провокационных фотографий, дающих неверные сведения о настоящем возрасте, или склонение к личной встрече с людьми, с которыми пользователь только что познакомился онлайн).

Благодаря технологиям web 2.0 пользователям стали доступны широкие интерактивные возможности, и важно помнить, что дети и подростки могут не только являться жертвами ненадлежащих активностей, но также сами могут инициировать или входить в состав антисоциальных или криминальных движений.

Безопасная социальная сеть: совместная работа всех заинтересованных сторон

Существует большой круг заинтересованных сторон, которые играют роль в управлении потенциальными рисками для детей и подростков. Среди них компании-провайдеры онлайн-услуг, государственные органы, родители, учителя, пользователи и неправительственные организации.

В настоящий момент опыт управления потенциальными рисками и злоупотреблениями различными аспектами Интернета показывает, что наиболее эффективным для подходом являются консультации и совместная работа заинтересованных сторон друг с другом в сочетании с исполнением принятых на себя обязательств.Данные принципы пропогандируют совместную работу заинтересованных стороны как наиболее эффективный способ управления потенциальными рисками соцсетей.

Компании-провайдеры соцсетей, позволяющие детям и подросткам подписываться на свои сервисы и услуги наряду со взрослыми, несут ответственность за то, чтобы оградить свои ресурсы от потенциальных рисков и внедрить адекватные меры и инструменты для снижения этих рисков.Этот документ призван описать принципы, которыми компании-провайдеры должны руководствоваться для того, чтобы соответствовать этим обязательствам.

Для описания условий, для которых, составлены данные рекомендации, ниже описаны основные роли, которые играют заинтересованные стороны в продвижении онлайн-безопасности, и как компании-провайдеры соцсетей могут работать вместе с ними.

- **Родители, учителя и другие лица, воспитывающие детей и подростков:** играют важную роль в поддержании и повышении качества идущего сейчас диалога с детьми и подростками о ответственном поведении онлайн. Компании-провайдеры должны предоставлять специально отобранную под потребности аудитории, доступную и актуальную информацию и инструменты для помощи им в этом диалоге, а также искать различные способы взаимодействия с преподавателями, органами государственной власти и другими заинтересованными сторонами для создания ресурсов и других образовательных механизмов.

- **Государственные и общественные организации:** должны предоставлять детям и подросткам знания и навыки по безопасной работе в Интернете. Госорганы должны убедиться в том, что учебные материалы по электронной безопасности правильно отражают актуальные на данный момент интернет-сервисы. Они также должны обеспечить сотрудникам правоохранительных органов доступ к соответствующим тренингам, инструментам и ресурсам, необходимым для эффективной борьбы с криминальными действиями в сети. Различные государственные структуры должны работать совместно для того, чтобы обеспечить эффективность и результативность межинституциональных структур и активностей.

Особенно важно, чтобы все заинтересованные стороны, включая государственные и общественные организации, в полной мере понимали новые вызовы и возможности, которые появляются в быстро развивающемся онлайн-пространства.Компании- провайдеры могут предоставлять органам государственной власти всю необходимую для этого информацию и должны искать пути для работы с правительствами.

- **Полиция и другие силовые структуры:** должны обеспечить своим сотрудникам доступ к адекватным и подходящим для их работы тренингам, а к ресурсам, необходимым для расследования незаконного использования онлайн-сервисов и преследования виновных лиц. Провайдеры соцсетей и силовые структуры должны обмениваться имеющимися знаниями и в соответствии с законодательством совместно расследовать негативные онлайн случаи.

- **Гражданское общество:** само по себе и через такие организации, как агентства по защите детей, молодежные организации и профессиональные службы, должно работать совместно с компаниями-провайдерами соцсетей и государственными органами, включаясь в консультации, диалоги или рабочие группы, нацеленные на общие для всех игроков целевые аудитории и проблемы в сети. Социальные сети все больше используются организациями, занимающимися вопросами психического здоровья, социальной защиты и помощи, для работы с детьми и подростками онлайн. Этот процесс имеет потенциал привести к очень положительным результатам. Подобные организации должны всесторонне изучить вопрос о том, как лучше всего сохранить основные этические и профессиональные правила и практики в отношении благополучия клиента, конфиденциальности информации, компетентности, ответственности и неприкосновенности клиенты при работе онлайн.

- **Конечные пользователи:** взрослые, дети и подростки должны всегда уважать правила использования сервиса и/или рекомендации сообщества. Они должны правильно использовать справочные материалы, инструменты, настройки и механизмы обратной связи, разработанные для того, чтобы они могли сами влиять на управление сообществами, к которым они принадлежат.

III. Принципы безопасности в социальных сетях

1. Повышать осведомленность участников воспитательного процесса о принципах и настройках безопасности в Интернете: обучать родителей и учителей правилам интернет-грамотности, чтобы они владели достаточной информацией для передачи этих навыков детям

Компании-провайдеры должны создать прозрачные рекомендации и материалы для обучения, дающие детям и подросткам инструменты, знания и умения для безопасной работы с их сервисами.

Эти материалы должны быть представлены в доступном, легком для понимания и практическом формате (например, на страницах помощи и/или в местах, где пользователи принимают решение о том, как им использовать данный сервис).

Сервис-провайдеры должны предоставить понятную информацию о том, что является неуместным поведением. Эта информация должны быть легко доступна и описывать последствия нарушения этих правил. Провайдеры должны разрабатывать другие способы предоставления этой информации за рамками правил работы сервиса.

Родители играют ключевую роль в обеспечении безопасности детей в Интернете, и эту роль лучше всего осуществить, когда они могут обсудить проблемы безопасности со своими детьми в открытом и информативном ключе.Провайдеры должны предлагать родителям ссылки, образовательные материалы и другие технические средства управления, которые служат для установления обучающего диалога, доверия и вовлеченности между родителями и детьми об ответственном и безопасном использовании Интернета.

Учителя и другие лица, отвечающие за защиту детей, также играют ключевую роль в продвижении безопасного использования соцсетей детьми.Компании-провайдеры должны быть уверенными в том, что материалы также дают возможность учителям помогать детям использовать соцсети безопасно и ответственно.

2. Стремиться к тому, чтобы интернет-продукты соответствовали потребностям и учитывали возрастную специфику пользователей, потребляющих эти продукты, согласно “Правилам использования” и “Пользовательскому соглашению”, разрабатываемым специально для каждого продукта

Провайдеры в повседневной разработке и управлении своих сервисов должны учесть, как их ресурсы могут быть связаны с потенциальными рисками для детей и молодежи и в какой степени молодые люди могут использовать эти сервисы.Сервис-провайдеры должны определить границу для потенциально неподходящего содержимого и контактов. Меры, которые доступны или подходят для каждого сервиса, будут различаться в каждом из случаев, но могут включать следующее:

- Четкое определение того, предназначены или нет сервисы для детей и подростков, а также определение минимального возраста для регистрации;
- применение мер для определения и удаления из сервисов пользователей, не достигших установленного возраста;
- применение мер для предотвращения попыток повторной регистрации с указанием другого возраста, если пользователи ранее не были допущены из-за того, что возраст был ниже минимально возможного (если правила требуют превышения минимального возраста), например, с помощью cookies;
- работа с техническими и законодательными ограничениями для продвижения соответствия минимальным требованиям по возрасту;
- продвижение понятия родительского контроля, который позволяет родителям контролировать использование сервисов своими детьми;
- предоставление средств контент-провайдерам, партнерам или пользователям, с помощью которых они смогут помечать, ранжировать или устанавливать возрастные ограничения контента там, где это применимо;
- демонстрация определенного профессионально произведенного контента только в определенное время суток.

3. Предоставлять пользователям технологии безопасности в Интернете

Провайдеры должны внедрять инструменты и технологии, с помощью которых дети и молодежь могут управлять своим опытом на сервисе, в частности в аспектах, связанных с работой с нежелательным (но не незаконному) контентом или поведением.Сервис-провайдеры должны оценивать, какие реализация каких мер имеет смысл, на основании сервисов, которые предлагаются для целевой аудитории.

Меры, которые могут помочь минимизировать риск нежелательных или неправильных контактов детей и молодежи с взрослыми, к примеру, включают в себя:

- обеспечение отсутствия профилей зарегистрированных пользователей младше18 лет в результатах поиска;
- установка по умолчанию всего профиля в скрытый режим или с установками, при которых необходимо вручную подтверждать список контактов для зарегистрированных пользователей младше 18 лет (некоторые сервис-провайдеры устанавливают профиль по умолчанию в скрытый режим для всех пользователей);
- обеспечение настроек профиля в скрытом режиме означает, что весь профиль не может быть просмотрен, а с пользователем никто не может связаться, кроме друзей из списка контактов (пользователи могут изменять настройки публичности и т. п.);
- предоставление пользователям возможности управлять доступом к их профилю, например, возможности запрещать пользователям просматривать профиль, и отклонять предложения дружбы;

- предоставление пользователям настройки, которая позволяет публикацию комментариев и содержимого в их профиле только прямым друзьям, а также удаление нежелательных комментариев;
- предоставление пользователям настройки для предварительной модерации комментариев других пользователей перед публикацией в своем профиле;
- предоставление пользователям легких в использовании инструментов, с помощью которых можно сообщить о контакте, нарушающем правила, или о неуместном поведении другого пользователя;
- обучение родителей различным инструментам для более широкого доступа в Интернет (например, рассказ о преимуществах использования инструментов фильтрации и/или родительского контроля) и инструментам, которые предоставляют родителям информацию и советы на сайтах социальных сетей для помощи в защите молодых людей.

4. Обеспечивать пользователей простыми механизмами уведомления о незаконном контенте или о контенте, нарушающем "Правила сообщества", разработанные для этого продукта

Провайдеры должны предоставить механизм для сообщения о некорректном контенте,нежелательном контакте или поведении, которые описаны в правилах работы сервиса, политике допустимого использования и/или рекомендациях сообщества. Эти механизмы должны быть легко доступны для пользователей, а процедура должна быть легка для понимания и соответствовать возрасту пользователей.

Подобные сообщения от пользователей должны быть обработаны, а реакция должна быть быстрой.

Пользователям должна предоставляться информация, которая необходима им для создания эффективного сообщения, а также описание процедуры обработки их запросов.

5.Реагировать на жалобы и уведомления пользователей

По получении извещения о предполагаемом нежелательном контенте или поведении у провайдеров должны быть в наличии эффективные процессы, которые применяются для быстрого просмотра и удаления проблемного содержимого.

Сервис-провайдеры должны обладать отработанными процедурамидля предоставления информации о нелегальном содержимом или поведении в соответствующие силовые структуры и/или на горячие линии.Эти процедуры зависят от местной юрисдикции и применяемого законодательства, а также существования эффективных средств сообщения подобной информации.

Провайдеры могут рассмотреть возможность включения ссылок на другие местные агентства или организации, например, на соответствующие сервисы помощи (InHope) и законодательные силовые структуры.Когда

безопасность или жизнь пользователей находится под угрозой, может быть принято решение связаться с экстренными службами, например, с помощью звонка на номер 999 (Соединенное Королевство) или 112 (ЕС).

Принцип 6. Предлагать пользователям инструменты для обеспечения безопасности персональных данных в Интернете

Провайдеры должны предоставлять пользователям ряд настроек приватности вместе с соответствующей информацией, которая будет поощрять их принимать взвешенные решения о том, какую информацию следует публиковать онлайн.Эти настройки должны занимать заметное место в работе пользователя и быть доступными на протяжении всего времени присутсвия пользователей онлайн.

Провайдеры должны оценить последствия автоматического сбора информации, предоставляемой во время регистрации в профилях, заставлять пользователей задуматься о последствиях раскрытия этой информации, когда необходимо, а также предоставить пользователям возможность редактировать и делать публичной/приватной такую информацию, когда это необходимо.

Пользователи должны иметь возможность видеть свой статус приватности или настроек в отдельно взятый период времени.Где возможно, настройки приватности пользователя должны быть видимы постоянно.

7. Оценивать и модернизировать средства и инструменты для выявления нелегального или запрещенного контента.

В ходе разработки и управления соцсетями компании-провайдеры должны определить потенциальные риски, применимые к данному сервису, для детей и молодежи в целях определения соответствующих процедур при обработке отчетов об изображениях, видео и тексте, которые могут содержать неуместное/недопустимое/запрещенное содержимое и/или поведение.

Существует ряд процедур, которые могут быть применены для приведения в соответствие с правилами работы сервиса, политикой допустимого использования и/или внутренними правилами. Они могут включать:

- пользовательские и/или автоматические формы модерации;
- технические инструменты (например, фильтры), для того чтобы пресечь распространение нелегального или запрещенного содержимого;
- оповещения внутри сообщества;
- сообщения, составляемые пользователями.

Некоторые провайдеры используют модераторов, которые взаимодействуют в реальном времени с детьми или молодежью.Такие провайдеры должны предпринимать обоснованные шаги (работать в рамках установленных практик, где возможно, или с применением закона, если применимо) для минимизации риска трудоустройства кандидатов, которые могут не подходить для работы, связанной с контактами в реальном

времени с детьми или молодыми людьми.

Различные сервисы имеют различные форматы профилей, которые позволяют пользователям предоставлять общий доступ к личной информации, например, некоторые провайдеры поощряют создание псевдонимов и публикацию аватаров и создание новых онлайновых личностей.Эти форматы отличаются от сайта к сайту.

IV. Оценка принципов безопасности социальных сетей

Провайдеры, поддерживающие эти принципы, выполняют практики по обеспечению безопасности и поддерживают все семь принципов, описанные в этом документе. Эти провайдеры оценивают риск потенциального вреда детям и молодежи при использовании сервиса и соответствующим образом учитывают применение специфических рекомендаций, описанных в настоящем документе.

- В интересах прозрачности эти провайдеры самостоятельно декларируют, каким образом они применяют принципы, которые относятся к их сервисам. Эти провайдеры предоставляют Европейской комиссии документ с собственной декларацией.
- Провайдеры делают доступной для публикации неконфиденциальную информацию из своих деклараций о применении ими данных принципов.
- Провайдеры, поддерживающие эти принципы, собираются через восемнадцать месяцев с другими заинтересованными сторонами для:
    - пересмотра тенденции в политиках безопасности и практиках;
    - информирования заинтересованных сторон об обновлениях в вопросах эволюции технологий коммуникации;
    - рассмотрения поведения пользователей и связанных рисков для пользователей;
    - обзора и редактирования документа для того, чтобы он соответствовал своему предназначению и был актуальным, а также отражал разработки в практике онлайн-безопасности;
    - оценки эффективности документа.
    - Провайдеры, поддерживая эти Принципы, и другие заинтересованные стороны работают вместе над поощрением других провайдеров социальных сетей поддержатьэтот документ и его положения. Они также стараются поднять уровень информированности об целях документа, вызывая широкий интерес у заинтересованных сторон, включая пользователей.

V. Приложение I

Пояснение, как эти принципы могут быть применены к приложениям

Как было указано во введении, приложения являются все большей частью социальных сетей. Существует три категории приложений, которые определяются отношениями, существующими между приложением и соцсетью. Эти отношения определяют, как провайдер может применять эти принципы, а именно:

1. Предустановленные приложения, интегрированные в соцсеть или спонсируемые соцсетью и предоставляемые в общий доступ провайдером соцсети.В этих случаях возможны отношения между соцсетью и разработчиком приложения. В этой категории приложений провайдеры должны :

- гарантировать оценку рисков потенциального вреда детям и молодежи, ставя своей целью соответствовать политикам и правилам безопасности сервиса;
- включать подходящие советы для детей и молодых людей в справочные материалы (например, в раздел «Справка»);
- Реагировать на сообщения о несоответствии приложения правил и политик сайта.

2. Приложения, которые были созданы сторонними разработчиками и которые отображаются в открытой API-платформе соцсети.Пользователи соцсети могут решить, установить такие приложения в свои профили или нет.Обычно в таких случаях отношения между соцсетью и разработчиком приложения ограничены. В этой категории приложений провайдеры должны:

- предпринимать разумные усилия для того, чтобы поднять осведомленность сторонних разработчиков о позитивных примерах и практиках работы (включая эти принципы и похожие инициативы);
- включать подходящие советы для детей и молодежи в справочные материалы (например, в раздел «Справка») и убедиться, что пользователи знают о том, что приложения сторонних производителей могут не предоставлять тот же уровень защиты, как и соцсети;
- по получении уведомления о том, что приложение, доступное для детей и молодежи, нарушает политику провайдера, провайдер соцсети должен, где это применимо, уведомлять производителя об этой ситуации и все время оставлять за собой право убрать приложения, которые нарушают политики провайдера.

3. Приложения, которые доступны от сторонних разработчиков на платформе, отличных соцсетей.Пользователи соцсети могут решить, устанавливать такие приложения в свои профили или нет.Обычно в таких случаях отношения между соцсетью и разработчиком приложения отсутствуют. В этой категории приложений, провайдеры должны:

- включать подходящие советы для детей и молодежи в справочные материалы (например, в раздел «Справка») и убедиться, что пользователи знают о том, что приложения

сторонних производителей могут не предоставлять тот же уровень защиты, как и соцсети;
- по получении уведомления о том, что приложение, доступное детям и молодежи, нарушает политики провайдера, провайдер соцсети будет, где это применимо и возможно, удалять ссылку на приложение.

1. **VI. Приложение II. Форма самодекларации**

Форма самодекларации принципов безопасной социальной сети ЕС

В интересах прозрачности провайдеры, поддерживающие принципы безопасной социальной сети ЕС, соглашаются провести самодекларацию, как было решено в принципах относительно социальных сетей, которые они предлагают, с помощью расположенной ниже формы.

1. О социальной сети (сетях)

Ниже следует краткое изложение декларации [название компании], включая краткое описание сервисов, которые она предлагает и которые подпадают в категорию «социальные сети», как описано в принципах.

2. Как компания рассматривает эти сервисы относительно принципов?

Ниже указано описание того, как [компания] учитывает принципы безопасной социальной сети ЕС в отношении своей социальной сети (социальных сетей).Данный раздел будет состоять из ссылок на рекомендации, приведенные в документе с принципами, где они применимы и где описывается, как их применять.

1. Повышать осведомленность участников воспитательного процесса о принципах и настройках безопасности в Интернете: обучать родителей и учителей правилам интернет-грамотности, чтобы они владели достаточной информацией для передачи этих навыков детям;
2. **Стремиться к тому, чтобы интернет-продукты соответствовали потребностям и учитывали возрастную специфику пользователей, потребляющих эти продукты, согласно “Правилам использования” и “Пользовательскому соглашению”, разрабатываемым специально для каждого продукта;**
3. **Предоставлять пользователям технологии безопасности в Интернете;**
4. **Обеспечивать пользователей простыми механизмами уведомления о незаконном контенте или о контенте, нарушающем “Правила сообщества”, разработанные для этого продукта;**
5. **Реагировать на жалобы и уведомления пользователей;**
6. **Предлагать пользователям инструменты для обеспечения безопасности персональных данных в Интернете;**
7. **Оценивать и модернизировать средства и инструменты для выявления нелегального или запрещенного контента.**

3. Другая информация

Данный раздел предоставляет описание любой другой информации, которая относится к тому, как компания учитывает настоящие принципы.