Принято

на педагогическом совете школы
«25» 05 2021 г., протокол № 18

Утверждено

Приказ от «__» ____ 20__ г. №____
Директор МБОУ СОШ № 21

_____ И.А. Барт

ПОЛОЖЕНИЕ
О порядке мониторинга социальных сетей по выявлению фактов распространения информации, склоняющей обучающихся к асоциальному поведению

1. Общие положения

1.1. Положение об осуществлении мониторинга учащихся в социальных сетях (далее - Положение) регламентирует порядок осуществления мониторинга учащихся образовательной организации в социальных сетях с целью организации мероприятий по профилактике негативных явлений в общеобразовательном учреждении (далее – ОУ).

1.2. Настоящее Положение разработано в соответствии с:

- Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;
- Федеральным законом от 29.12. 2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;
- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности»;
- Федеральным законом от24 июня 1999 №120 – ФЗ «Об основах системы профилактики безнадзорности правонарушений несовершеннолетних»;
- иными нормативно-правовыми актами Российской Федерации;

1.3. Используемые понятия:

1.3.1. социальная сеть - сайт в информационно-телекоммуникационной сети «Интернет» (далее - сеть «Интернет»), предназначенный для распространения, передачи в сети «Интернет» пользователями социальной сети (далее - пользователь, пользователи) информации, голосовой информации, письменных текстов, изображений, звукозаписей, музыкальных произведений, аудиовизуальных произведений и для удаленного взаимодействия, иного обмена информацией между пользователями.

1.3.2. мониторинг учащихся ОУ в социальных сетях (далее – мониторинг) – деятельность работников и родителей (законных представителей) несовершеннолетних учащихся (далее – субъекты осуществления мониторинга), направленная на выявление негативных явлений, проявляющихся в информации, распространяемой учащимися в социальных сетях:

- определение круга пользователей социальными сетями из числа обучающихся образовательной организации, зарегистрированных в социальной сети под своим именем;

- выявление из числа условных лидеров (наиболее популярных пользователей);

- выявление признаков девиантного поведения пользователей, указанной категории;

- выявление признаков, указывающих на возможности наркотизации исследуемого круга пользователей социальной сетью.

Возможные Социальные сети, в которых могут быть зарегистрированы дети «Вконтакте», «Одноклассники», «Facebook», «Фотострана», «MySpace», «instagram», «Мой Мир», «ДругВокруг», на почтовом сайте mail.ru.

1.4. Мониторинг учащихся ОУ в социальных сетях осуществляется в рамках работы ОУ по профилактике девиантного поведения среди учащихся.

2. Направление мониторинга

2.1 К информации, запрещенной для распространения среди детей, относится информация:

- побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству;

- способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и содержащую алкоголь продукцию, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;

- обосновывающая или оправдывающая допустимость насилия и (или) жестокости, либо побуждающая осуществлять насильственные действия по отношению к людям, или животным, за исключением случаев, предусмотренных настоящим Федеральным законом;

- отрицающая семейные ценности, пропагандирующая нетрадиционные сексуальные отношения и формирующая неуважение к родителям и (или) другим членам семьи;

- оправдывающая противоправное поведение;

- содержащая нецензурную брань;

- содержащая информацию порнографического характера;

- пропагандирующею фашизм, национализм, экстремизм;

- о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), включая фамилии, имена, отчества, фото- и видеоизображения такого несовершеннолетнего, его родителей и иных законных представителей, дату рождения такого несовершеннолетнего, аудиозапись его голоса, место его жительства или место временного пребывания, место его учебы или работы, иную информацию, позволяющую прямо или косвенно установить личность такого несовершеннолетнего.

3. Организация мониторинга учащихся ОУ в социальных сетях

3.1. Мониторинг осуществляется работниками, к которым относятся: руководители, педагогические работники (далее – субъекты мониторинга).

3.2. Мониторинг может осуществляться родителями (законными представителями) несовершеннолетних учащихся в отношении своих детей.

3.3. Мониторинг осуществляется на основе данных, получаемых субъектами осуществления мониторинга в социальных сетях, расположенных в сети «Интернет», к которым могут относиться: Вконтакте, Одноклассники, Facebook, Фотострана, MySpace, Instagram, Twitter, «Мой Мир» на почтовом сайте mail.ru, а также переписка в мессенджерах - WhatsApp, Viber, FacebookMessenger, Skype, ICQ, GoogleHangouts, Telegram, Snapchat, Discord и др.

3.4. Мониторинг осуществляется субъектами мониторинга раз в месяц не позднее 20-го числа.

3.5. В случае выявления субъектами мониторинга в социальных сетях, расположенных в сети «Интернет», информации, указанной в п. 2 настоящего Положения, которая распространяется учащимися, субъекты мониторинга незамедлительно сообщают о выявленных фактах в администрацию ОУ.

3.6. Факт выявления информации, указанной в п. 2 настоящего Положения, субъект мониторинга фиксирует в форме служебной записки, в которой указываются электронные ссылки на социальные сети, расположенные в сети «Интернет», приложением к которой являются скриншоты соответствующих изображений.

3.7. В случае выявления родителями (законными представителями) несовершеннолетнего учащегося ОУ в социальных сетях, расположенных в сети «Интернет» информации, указанной в п. 2 настоящего Положения, которая распространяется их ребенком, родители (законные представители) несовершеннолетнего учащегося сообщают о выявленных фактах работнику ОУ – классному руководителю, у которого обучается их ребенок. Классный руководитель фиксирует информацию в форме служебной записки сообщает администрации ОУ, в которой указываются электронные ссылки на социальные сети, расположенные в сети «Интернет», приложением к которой являются скриншоты соответствующих изображений.

4. Действия специалистов образовательных организаций по подготовке и проведению мониторинга социальных сетей

4.1. Необходимо определить изучаемых лиц на страничке в социальной сети, содержание которых подлежит анализу.

4.2.При анализе страницы необходимо обратить внимание на:

- Наличие терминологии, используемой в среде потребителей наркотических средств и психотропных веществ.
- Выражение гнева, ненависти, безразличия, жестокости, наличие групп с агрессивными концепциями, склоняющих к противоправным действиям и т.п.

- Окружение и друзей подростка. Возможно, уже знакомых «неблагополучных» детей или взрослых сомнительного вида.

- Профиль в социальной сети представляет собой страничку с разветвленной структурой, он является идентификатором каждого пользователя.

- Профиль содержит информацию о друзьях пользователя, группах (сообществах), в которые он входит, фотографии, аудиозаписи, видеозаписи и др.

- Каждая страница пользователя содержит комментарии на так называемой «стене». Комментарии характеризуют круг интересов, увлечений, актуальных на данный момент проблем, манеры общения в сети.

5. Результаты мониторинга

5.1 Результаты, полученные в ходе мониторинга профилей обучающихся, могут иметь большое значение при организации воспитательной работы с подростками и юношеством в конкретной группе, учебном заведении.

5.2 При обнаружении на изученных страничках пользователей информации сомнительного содержания или окружение и друзей подростка. сомнительного вида необходимо поставить в известность заместителя директора по ПР образовательной организации.

Приложение

Общая безопасность в интернете.

В первую очередь это действия мошенников, которые хотят получить финансовую или иную выгоду. Мошенники могут быть хорошо оснащены и использовать самые разные инструменты и методы — например, вирусное программное обеспечение (далее — вирусы), поддельные сайты, мошеннические письма, перехват и подбор паролей к учетным записям в социальных сетях и почтовых сервисах.

Вирусы.

Вирусы могут распространяться с помощью вложенных файлов и ссылок в электронных письмах, в сообщениях в социальных сетях, на съемных носителях, через зараженные сайты. При этом сообщение с вирусом может быть получено как от постороннего человека, так и от знакомого, но уже зараженного участника социальной сети или почтовой переписки. Зараженными могут быть сайты, как специально созданные в целях мошенничества, так и обычные, но имеющие уязвимости информационной безопасности.

Рекомендации:

Использовать антивирусное программное обеспечение с обновленными базами вирусных сигнатур.

Не открывать вложенные файлы или ссылки, полученные по электронной почте, через социальную сеть или другие средства коммуникаций в интернете, не удостоверившись, что файл или ссылка не содержит вирус.

Внимательно проверять доменное имя сайта (например, www.yandex.ru), так как злоумышленники часто используют похожие имена сайтов, чтобы ввести жертву в заблуждение (например, www.yadndex.ru).

Обращать внимание на предупреждения браузера или поисковой машины о том, что сайт может угрожать безопасности компьютера.

Не подключать к своему компьютеру непроверенные съемные носители.

Не поддаваться на провокации злоумышленников, например, с требованием перевести деньги или отправить SMS, чтобы снять блокировку компьютера.

Мошеннические письма.

Злоумышленники могут использовать различные методы социальной инженерии (угрозы, шантаж, игру на чувствах жертвы — например, жадности или сочувствии), чтобы выманить деньги. В таких случаях они пишут письма определенного сценария. Один из примеров — так называемые «нигерийские письма», в которых автор обещает жертве огромную прибыль взамен на небольшие накладные расходы.

Рекомендации:

Внимательно изучить информацию из письма. Проверить достоверность описанных фактов. Если в письме предлагается большая выгода за незначительное вознаграждение, скорее всего, оно мошенническое.

Игнорировать такие письма.

Получение доступа к аккаунтам в социальных сетях и других сервисах.

Злоумышленники часто стремятся получить доступ к аккаунтам жертвы, например, в социальных сетях, почтовых и других сервисах. Украденные аккаунты они используют, например, для распространения спам-писем и вирусов.

Мошенники могут получить доступ к учётной записи следующими способами:

Заставить ввести свои данные на поддельном сайте.

Подобрать пароль, если он не является сложным.

Восстановить пароль с использованием "секретного вопроса" или введенного ящика электронной почты.

Перехватить пароль при передаче по незащищенным каналам связи.

Как правило, для кражи данных об аккаунтах используются фишинговые сайты. **Фишинг** (англ. phishing, от fishing — рыбная ловля, выуживание) — вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Злоумышленники создают фишинговые сайты, копирующие интерфейс известных ресурсов, а жертвы вводят на них свои логины и пароли, не понимая, что сайты поддельные.

Рекомендации:

Использовать сложные пароли (сложные пароли состоят как минимум из 10 символов, включают буквы верхнего и нижнего регистра, цифры и специальные символы, не содержат имя пользователя и известные факты о нем).

Никому не сообщать свой пароль.

Для восстановления пароля использовать привязанный к аккаунту мобильный номер, а не секретный вопрос или почтовый ящик.

Не передавать учетные данные — логины и пароли — по незащищенным каналам связи (незащищенными, как правило, являются открытые и общедоступные wi-fi сети).

Внимательно проверять доменные имена сайтов, на которых вводятся учетные данные.

Правило 1. Установите вместе с детьми четкие правила посещения сайтов. Определите, какие сайты они могут посещать, какие – посещать нельзя. Выберите сайты, которые можно посещать вашему ребенку, и заблокируйте доступ к неподходящим материалам. Настройте параметры безопасности вашего компьютера.

Правило 2. Помогите детям выбрать правильное регистрационное имя и пароль. Убедитесь в том, что они не содержат никакой личной информации.

Правило 3. Объясните детям необходимость защиты их конфиденциальности в сети Интернет. Настаивайте на том, чтобы они никогда не выдавали своего адреса, номера телефона или другой личной информации; например, места учебы или любимого места для прогулки.

Правило 4. Не позволяйте ребенку встречаться с онлайн-знакомыми без разрешения. Если ребенок желает встретиться с новым интернет-другом, следует настоять на сопровождении ребенка на эту встречу.

Общение в Интернете может повлечь за собой коммуникационные риски, такие как незаконные контакты (например, груминг, кибербуллинг и др.). Даже если у большинства пользователей чат-систем (веб-чатов или IRC) добрые намерения, среди них могут быть и злоумышленники. В некоторых случаях они хотят обманом заставить детей выдать личные данные, такие как домашний адрес,

телефон, пароли к персональным страницам в Интернете и др. В других случаях они могут оказаться преступниками в поисках жертвы. Специалисты используют специальный термин «груминг», обозначающий установление дружеских отношений с ребенком с целью вступления в сексуальный контакт. Знакомство чаще всего происходит в чате, на форуме или в социальной сети от имени ровесника ребенка. Общаясь лично («в привате»), злоумышленник входит в доверие к ребенку, пытается узнать личную информацию и договориться о встрече.

Кибербуллинг — преследование сообщениями, содержащими оскорбления, агрессию, запугивание, хулиганство, социальное бойкотирование с помощью различных интернет-сервисов. Предупреждение кибербуллинга: Объясните детям, что при общении в Интернете они должны быть дружелюбными с другими пользователями, ни в коем случае не писать грубых слов – читать грубости также неприятно, как и слышать. Научите детей правильно реагировать на обидные слова или действия других пользователей. Объясните детям, что нельзя использовать Сеть для хулиганства, распространения сплетен или угроз. Старайтесь следить за тем, что ребенок делает в Интернете, а также следите за его настроением после пользования Сетью.

Правило 5. Научите детей уважать других в Интернете. Убедитесь, что они знают о том, что правила хорошего поведения действуют везде – даже в виртуальном мире.

Правило 6. Настаивайте, чтобы дети уважали собственность других в Интернете. Объясните, что незаконное копирование и использование чужой работы – текста, музыки, компьютерных игр и других программ – является кражей.

Приложение

Рекомендации обеспечения безопасности учащихся в Интернете.

Поговорите с учащимся о безопасности в Интернете. Объясните основные правила, возможности различных технологий и последствия нарушений. Самое главное: убедите, что в любой непонятной или пугающей ситуации ему следует обращаться к педагогам, чтобы найти безопасное решение.

1. **Используйте компьютер и смартфон вместе с детьми**. Это хороший способ научить их правилам безопасности в Интернете. При этом дети поймут, что решать возможные проблемы лучше всего вместе.
2. **Расскажите детям больше о сайтах и сервисах в Интернете**. Поговорите о том, что их интересует в Интернете и какие страницы им можно посещать.
3. **Безопасные пароли**. Помогите своей семье приобрести правильные привычки в отношении паролей. Расскажите об их использовании. Напомните, что пароли никому нельзя передавать, за исключением лиц, которым можно доверять, например, родителям. Убедитесь, что у детей вошло в привычку выходить из своих аккаунтов, когда они используют общественные компьютеры в школе, кафе или библиотеке.
4. **Используйте настройки конфиденциальности и управления доступом**. В Интернете немало сайтов, на которых можно публиковать свои комментарии, фото и видео, рассказывать о том, что с вами произошло, как вы живете и т. д. Обычно такие сервисы позволяют определить уровень доступа к вашей информации ещё до ее публикации. Поговорите с членами своей семьи и определите, о чем не следует рассказывать всем. Научите детей уважать конфиденциальность друзей и родных.
5. **Проверьте возрастные ограничения**. Многие онлайн-сервисы, в том числе Google, предоставляют доступ ко всем функциям только совершеннолетним. А создавать аккаунты Google могут только пользователи не моложе 13 лет. Прежде чем ваш ребенок зарегистрируется на том или ином сайте, самостоятельно проверяйте условия его использования и соответствие материалов правилам, принятым в вашей семье.
6. **Научите детей ответственному поведению в Интернете**. Помните золотое правило: то, что вы не сказали бы человеку в личном общении, не стоит отправлять ему по SMS, электронной почте, в чате или комментариях на его странице. Поговорите с детьми о том, как другие могут воспринимать их слова, и разработайте для своей семьи правила общения.
7. **Посоветуйтесь с другими взрослыми**. Привлеките к обсуждению этой темы друзей, родственников и коллег. Другие родители и специалисты по работе с детьми могут оказать вам неоценимую помощь в том, как научить детей и родственников правильному использованию самых разных информационных технологий.
8. **Защитите свой компьютер и личные данные**. Используйте антивирусное программное обеспечение и регулярно его обновляйте. Поговорите со своей семьей о типах личной информации – например, номер социального страхования, номер телефона или домашний адрес – эти данные не должны быть размещены в Интернете. Научите свою семью не принимать файлы или открывать вложения в электронной почте от неизвестных людей.

9. **Не останавливайтесь на достигнутом**. Безопасность в Интернете требует постоянного внимания, поскольку технологии непрерывно совершенствуются. Старайтесь всё время держать руку на пульсе. Пересматривайте правила пользования Интернетом в семье, следите за тем, как ваши близкие осваивают новые технологии, и время от времени давайте им советы. Вредоносные программы (вирусы, черви, «троянские кони», шпионские программы, боты и др.) могут нанести вред компьютеру и хранящимся на нем данным. Они также могут снижать скорость обмена данными и даже использовать ваш компьютер для распространения вируса, рассылать от вашего имени спам с адреса электронной почты или профиля какой-либо социальной сети.

Как настроить родительский контроль в Google Play

Чтобы ограничить покупку и скачивание контента в приложении "Play Маркет", вы можете включить родительский контроль.

Чем полезен родительский контроль

По умолчанию все, кто пользуется устройством, могут скачивать и покупать контент с любым возрастным ограничением. Включив родительский контроль, вы запретите доступ к определенному контенту.

Примечание. Запрещенный контент будет по-прежнему доступен по прямой ссылке.

Как настроить родительский контроль

Настроив родительский контроль, вы можете отключать и включать его. Все выбранные параметры сохраняются, поэтому их не нужно настраивать заново при повторном включении функции или смене PIN-кода. Благодаря этому вы сможете быстро включить родительский контроль и отдать устройство ребенку, а затем отключить фильтры, когда он вернет его.

1. Откройте приложение "Play Маркет" ▶ на устройстве Android.
2. В левом верхнем углу экрана нажмите на значок меню ☰ и выберите **Настройки > Родительский контроль**.
3. **Включите** функцию.
4. Ограничьте доступ к настройкам родительского контроля, установив PIN-код. Желательно, чтобы другие пользователи устройства его не знали.
5. Установите фильтры.

- **Приложения, игры, фильмы и сериалы.** Выберите максимально допустимое возрастное ограничение для скачиваемого и покупаемого контента.
- **Музыка и книги.** Запретите или разрешите скачивание и покупку контента для взрослых.

6. Родительский контроль действует только на том устройстве, где вы его астроили. При необходимости включите его на другом устройстве, снова выполнив приведенные выше инструкции. Также учтите, что если на устройство добавлено несколько пользователей, для них можно установить разные фильтры.

Примечание. Родительский контроль с фильтрами для отдельных типов контента доступен не во всех странах. Например, если вы путешествуете в регионе, где функция не поддерживается, она начнет работать, только когда вы вернетесь домой.

Как работает родительский контроль

Родительский контроль по-разному фильтрует приложения, игры, музыку, фильмы, сериалы и книги. Чтобы узнать подробную информацию, прочитайте разделы ниже.

При настройке родительского контроля для приложений и игр вы можете установить максимально допустимое возрастное ограничение. Покупать и скачивать контент с более высоким ограничением будет нельзя.

Однако при поиске приложений и игр или при переходе по прямым ссылкам вы все равно сможете увидеть запрещенный контент.

Примечание. Вам по-прежнему будут доступны приложения и игры, скачанные до настройки родительского контроля, даже если их возрастное ограничение выше максимального.

Как работает родительский контроль в **Play Играх**

Родительский контроль не распространяется на контент в Play Играх, в том числе на купленный и рекомендованный.

Если вы попытаетесь установить игру в этом приложении, откроется ее страница в Play Маркете.

На ней родительский контроль может запретить доступ.

При настройке родительского контроля для фильмов вы можете установить максимально допустимое возрастное ограничение. Покупать, брать напрокат и воспроизводить контент с более высоким ограничением будет нельзя.

Однако при поиске фильмов или при переходе по прямым ссылкам вы все равно сможете увидеть запрещенный контент.

Если возрастное ограничение фильмов, в том числе купленных или взятых напрокат, превышает максимально допустимое, они будут скрыты в Play Маркете и Play Фильмах.

Чтобы этот контент снова стал виден, отключите родительский контроль.

Приложение

Алгоритм работы для педагогов и законных представителей в сети Интернет, социальных сетях по выявлению деструктивных проявлений среди учащихся учреждений образования

1. Изучить материалы по обеспечению безопасности при использовании сети Интернет:
2. Организовать разъяснительную работу с родителями и учащимися по работе с интернет-ресурсами в безопасном режиме, по созданию форумов, блогов, групп, использованию специализированных программ.
3. Зарегистрироваться в социальных сетях.
4. Отправить запросы на добавление в друзья к своим учащимся.
5. Войти в группы, где зарегистрированы учащиеся.
6. Просматривать страницы учеников своего класса, отслеживая, с кем общаются, какие страницы посещают, отмечают, в каких группах состоят и т.д.
7. Создавать группы совместно с учениками, наполняя их интересным содержанием, вовлекая учащихся в полезное для их развития общение.
8. При выявлении случаев деструктивных проявлений среди учащихся (наличие на странице «подозрительных» групп, лайки на деструктивных форумах, фотографиях и др.):

- обратить внимание на поведение ребенка в школьной, классной среде;
- информировать педагога-психолога, инспекцию по делам несовершеннолетних;
- осуществлять индивидуальные разъяснительные беседы с учащимися, родителями.