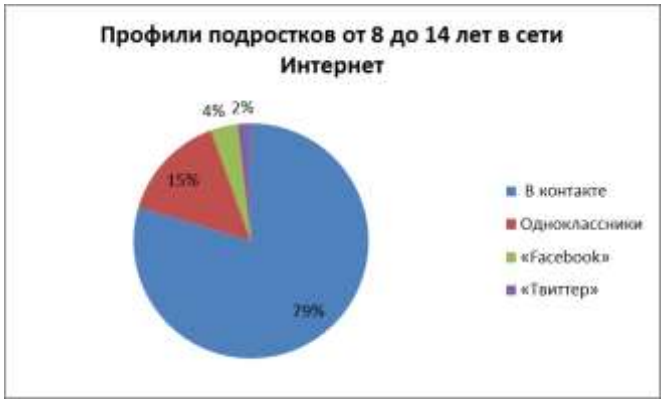
Предупреждение экстремистских проявлений в электронных СМИ (в Интернете)

Законодательно противодействие экстремизму осуществляется в соответствии с Федеральным законом от 25 июля 2002 г. «О противодействии экстремистской деятельности», согласно которому на территории Российской Федерации запрещаются распространение экстремистских материалов, а также их производство или хранение в целях распространения. В случаях, предусмотренных законодательством Российской Федерации, производство, хранение или распространение экстремистских материалов является правонарушением и влечет за собой ответственность. Несмотря на наличие законодательных норм необходимо познакомить детей с правилами поведения в сети интернет.

По данным, приведенным лабораторией Касперского, в России 4 миллиона детей в возрасте ***от 8 до 14 лет*** пользуются интернетом, из которых ***78%*** имеют личный профиль в социальных сетях.



У каждого 5–го ребёнка более ***100*** друзей в социальной сети;
40% детей после знакомства онлайн хотят перенести общение в реальную жизнь;
10% российских родителей знают о встречах своих детей с интернет-знакомыми.

По мнению родителей, ***88%*** из них знают о том, чем дети занимаются в интернете и какие сайты посещают, ***92%*** устанавливают для детей правила нахождения в Сети.

В действительности:

40% детей не обсуждают проблему безопасности в интернете с родителями

33% детей не рассказывают родителям о том, какие сайты посещают

34% родителей не устанавливают для детей никаких правил поведения в Сети

23% родителей жалуются, что дети слишком много времени проводят в интернете

14% родителей не представляют, сколько времени дети тратят на интернет.

В Интернете, как и в реальной жизни, подростков подстерегают опасности: доступность нежелательного контента в социальных сетях, анонимность, возможность скрыть свой реальный образ, розыгрыши призов, платные СМС на короткие номера и т. п. Наиболее опасные явления:

- Порнография, пропаганда насилия и экстремизма.
- Опасные знакомства.
- Обман и вымогательство денег.
- Заражение компьютера вредоносными программами.

Заражение компьютера вредоносными программами, не менее опасно, чем перечисленные выше угрозы. В результате вирусных атак информация, вводимая, сохраняемая на компьютере, может быть повреждена, уничтожена, переслана третьим лицам. Злоумышленникам может стать доступна информация и величине кредитного счета, пин-код и номер

кредитной карты. Информация, полученная в результате вирусного заражения, может быть использована для оказания психологического воздействия или в противоправных действиях по отношению к подростку и членам его семьи.

Нередко Интернет используется для дезинформации, которая подается как справедливый протест против ограничения на свободу выражения своего мнения и тяжелое положение лиц, являющихся политическими заключенными. Распространители экстремистской информации стараются вызвать симпатию у пользователей и привлечь на свою сторону. Для этой цели могут быть использованы данные, позволяющие идентифицировать отношение подростка к той или иной проблеме. Данные могут быть получены из личной информации, введенной в он-лайн анкету или бланк заявки, или похищенные путем взлома почтового ящика, анализа сайтов посещения и др.

В поиске наиболее восприимчивой аудитории, новых членов своих организаций вербовщики используют технологии веб-сайта (звук, видео и т.п.), он-лайн технологии (чаты, форумы). С подростками, которые кажутся наиболее заинтересованными или хорошо подходящими для выполнения асоциальной деятельности, злоумышленники входят в контакт.

Злоумышленники могут попросить о пожертвованиях посредством адресных рассылок по электронной почте, сообщений компьютерных вирусов, в чатах или на форумах.

Последствия бесконтрольного общения с интернетом для детей и подростков могут быть самыми непредсказуемыми и трагичными. Для того чтобы сделать интернет-жизнь более безопасной, необходимо познакомить учащегося с правилами поведения в Интернете:

♦ Нельзя разглашать ***пароль от своего почтового ящика*** или аккаунта (учетной записи), страницы в социальных сетях. В результате злоумышленники могут воспользоваться вашим адресом и вашей адресной книгой для рассылки сообщений, в том числе: спама, сообщений неприличного характера или экстремисткой направленности, совершения противоправных действий (мошенничества, угроз, психологического давления и др.) от вашего имени.

♦ ***Не стоит сохранять пароли на компьютере***, при вирусном заражении пароли могут быть похищены.

♦ ***Необходимо закрывать сессию*** (осуществлять выход) по завершению работы с аккаунтом Google, на странице в «Одноклассниках», «Вконтакте» и др. При работе на чужом компьютере, в общественном месте открытая сессия предоставляет доступ ко всей информации пользователя: сообщениям в социальной сети, фото, видео и документам, адресной книге.

♦ ***Нельзя оставлять в публичном доступе или отправлять незнакомцам по почте***, при общении в социальной сети или в чате контактную информацию – любой злоумышленник может выследить человека по его адресу или номеру телефона.

♦ ***Нельзя соглашаться на уговоры незнакомых людей о личной встрече***. Подобные предложения лучше игнорировать, а общение со слишком настойчивым человеком прекратить.

♦ ***Не надо публиковать адрес своей электронной почты ни на каких форумах***, сайтах сообществ и социальных сетей. Это может стать причиной спама.

♦ ***Не следует переходить по ссылкам в сообщениях от неизвестных адресатов***. Это небезопасно, поскольку сообщение может быть отправлено злоумышленниками. Тем более сообщать логин и пароль при переходе на другой сайт.

♦ ***Не стоит переходить по ссылкам в сообщениях с чрезмерно заманчивыми предложениями***, например, поднять «рейтинг» учетной записи или получить «супервозможности» в социальной сети. Чаще всего такие сообщения рассылают мошенники или злоумышленники для того, чтобы заманить пользователя на вредоносную веб-страницу или заразить его компьютер вирусом.

♦ ***Не стоит обращать внимания на предложение бесплатных подарков***, легкого заработка, сообщения о получении наследства и пр. Такие сообщения рассылают только мошенники. Поводом для вымогательства может стать и грант на обучение в престижном заведении, и участие в модельном агентстве.

Выход ребенка в интернет во много раз увеличивает риск заражения компьютера, которым он пользуется.

Поэтому стоит рекомендовать родителям использование встроенных в операционные системы и антивирусные программы решений безопасности:

- Фильтрация нежелательного веб-контента (ресурсов эротического, экстремистского содержания и ресурсов, пропагандирующих насилие).
- «Безопасный поиск» в большинстве популярных поисковых систем.
- Блокирование доступа ребенка к конкретным веб-сайтам.
- Блокирование доступа ребенка к группам для взрослых в социальных сетях.
- Возможность отслеживать переписку ребенка в социальных сетях и IM-чатах и ограничивать общение с подозрительными корреспондентами.
- Возможность установить запрет на пересылку любых персональных данных в социальных сетях и IM-чатах.
- Блокирование фишинговых и порносайтов, на которые часто ведут ссылки в сообщениях спамеров.
- Защита от спама.

В целом, общение и поведение в Интернете ничем не отличается от реальной жизни. Сохранение конфиденциальной информации, критическое отношение к заманчивым предложениям от посторонних лиц, избегание случайных контактов, соблюдение правил поведения учащимися, контроль со стороны взрослых за поведением детей и подростков и создание для них безопасной среды позволят уберечь не только учащихся от столкновения с опасными явлениями, но общество от экстремистских проявлений, как в Интернете, так и в жизни.

Глоссарий терминов, употребляемых в электронных СМИ и в интернете.

On-line – режим реального времени.

Аккаунт (учетная запись) – создается при регистрации на интернет–ресурсе (Google, «Одноклассники», «Вконтакте», Skype, ICQ и др) (аккаунт). На основании учетной записи происходит авторизация (идентификация) пользователя на данном ресурсе и пользователь получает возможность организовать собственную виртуальную среду на этом интернет-ресурсе. Для создания учетной записи необходимы логин и пароль.

Веб-форум – термин соответствует смыслу исходного понятия «форум». Форум предлагает набор тем для обсуждения. Работа форума заключается в создании пользователями сообщений для обсуждения внутри этих тем.

Контент – информационное содержание ресурса (текст, графика, мультимедиа).

Логин – имя, идентифицирующее пользователя, при обращении к Интернет-ресурсам.

Открытая сессия предоставляет доступ в режиме реального времени ко всей информации пользователя: сообщениям в социальной сети, фото, видео и документам, адресной книге. При работе на чужом компьютере, в общественном месте по завершении работы с сервисами Google (редактор сайтов, блогов, документов), страницами в «Одноклассниках», «Вконтакте» необходимо осуществить выход (закрыть сессию). В противном случае, так как сессия открыта, информация, размещенная на странице, может быть изменена,

удалена любым пользователем. При открытой сессии любой пользователь получает доступ к списку ваших контактов и может отправить любые сообщения.

Под словом чат обычно понимается групповое общение, хотя к ним можно отнести и обмен текстом «один на один» посредством программ мгновенного обмена сообщениями, например, XMPP, ICQ или даже SMS (источник Википедия).

Социальная сеть – веб-сервис или сайт в интернете, предназначенные для построения, отражения и организации социальных взаимоотношений.

Фишинг (англ. phishing, от fishing – рыбная ловля, выуживание – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям. Это достигается путём проведения массовых рассылок электронных писем, а также личных сообщений внутри различных сервисов, например, от имени банков (Ситибанк, Альфа-банк), сервисов (Rambler, Mail.ru) или внутри социальных сетей (Facebook, Вконтакте, Одноклассники.ru). В письме, например, от имени популярных брендов, помещается прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт, с которого происходит переадресация на другой (поддельный) сайт. После того, как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приёмами побудить пользователя ввести на поддельной странице свои логин и пароль, которые они использует для доступа к определенному сайту (например, интернет-банку, странице «Вконтакте»), что позволяет мошенникам получить доступ к аккаунтам и (или) банковским счетам.

Чат чаттер (англ. chatter – болтать) – средство обмена сообщениями по компьютерной сети в режиме реального времени, а также программное обеспечение, позволяющее организовывать такое общение. Характерной особенностью является коммуникация именно в реальном времени или близкая к этому, что отличает чат от форумов и других «медленных» средств.

Список ресурсов, которые могут быть использованы для предупреждения экстремистких проявлений в электронных СМИ (в Интернете):

- Асеев Е. Небезопасный интернет. https://www.securelist.com/ru/analysis/208050652/Nebezopasnyy_internet
- Википедия – свободная энциклопедия http://ru.wikipedia.org – 2012г.
- Компьютерная безопасность: мифы и реальность. Образовательные программы «Лаборатории Касперского». www.kasperskyacademy.com/ru/view.html?id=458
- Безопасность и конфиденциальность. Образовательные программы Microsoft. http://windows.microsoft.com/ru-RU/windows7/help/security-privacy-user-accounts