УДК 004.056

Безопасность несовершеннолетних в социальных сетях и сети Интернет

Кобякова Ю.А. (Южный федеральный университет, Институт компьютерных технологий и информационной безопасности, Кафедра информационно-аналитических систем безопасности, Таганрог, Россия)

Научный руководитель – Петряева М.В.

(Южный федеральный университет)

У открытого доступа к сети «Интернет» в современном мире есть не только положительные стороны. Информация, хранящаяся в виртуальном пространстве, может причинить вред нравственному и психологическому развитию подростка, а так же здоровью. В следствие стремительного развития рынка сотовой связи становится все более популярным мобильный Интернет.

Введение. У открытого доступа к сети «Интернет» в современном мире есть не только положительные стороны. Информация, хранящаяся в виртуальном пространстве, может причинить вред нравственному и психологическому развитию подростка, а так же нанести вред здоровью. В то же время становится все более популярным мобильный Интернет, в следствие стремительного развития рынка сотовой связи.

Основная часть. После проведения исследования Центром Безопасного Интернета, в России, было выявлено, что больше половины несовершеннолетних пользователей интернета посещают сайты, содержащие негативные данные: порносайты просматривают 39% детей, сцены насилия наблюдают 19%, 16% ребят увлекаются азартными играми, и 14% детей интересуются наркотиками и алкоголем. И несмотря на это, 90% родителей верят, что абсолютно держат под контролем все ресурсы, которые посещает их ребенок в сети «Интернет».

Уполномоченный при Президенте РФ по правам ребенка отмечает, что сейчас Россия занимает лидирующее в мире после США по распространению детской порнографии в Интернете. МВД Российской Федерации предоставляет данные о том, что Россия поставляет на рынок примерно 30% мирового объема детской порнографии. В последнее время число сайтов с детской порнографией увеличилось почти на треть от количества сайтов раньше, а объем соответствующего содержания поднялся в 25 раз. Число потребителей, регулярно приобретающих порнопродукцию с участием детей, оценивается в 800 тыс. человек. 44% несовершеннолетних пользователей Интернета хотя бы раз подвергались в сети сексуальным домогательствам.

Кибербуллингом в большинстве случаев служит отправка сообщений жертве с угрозами. Могут быть различные варианты угроз, например: публикации унижающих достоинство жертвы фотографий и видео в социальных сетях или создание поддельных веб-страниц с информацией, которая как-либо может унизить жертву

Кураторы "групп смерти" намеренно склоняют подростка к суициду, но делают это так ненавязчиво, что жертва этого не понимает. Им поэтапно присылают задания, последней целью которой является суицид.

Государство берет на себя ответственность за информационный контент, к которому несовершеннолетние могут получить доступ. В России существует закон № 436-ФЗ от 29 декабря 2010 года "О защите детей от информации, причиняющей вред их здоровью и развитию" устанавливает правила безопасности медиа-данных детей при обороте на территории России продукции СМИ, печатной, аудиовизуальной продукции на любых видах носителей, программ для компьютеров и баз данных, а также информации, размещаемой в информационно-телекоммуникационных сетях.

Выводы. Чтобы предотвратить кражи личных данных, взломы страниц в социальных сетях, оскорбления несовершеннолетних незнакомцами, стоит придерживаться нескольких правил. Некоторые из правил обязаны выполнять и сами взрослые, такие как:

- Осведомлять несовершеннолетних о безопасности в интернете, о кибербуллинге, про фишинговые сайты и т.п.,
- Родители должны контролировать время проведения в интернете подростка и его действия (существуют приложения для родительского контроля как на компьютерах, так и на мобильных устройствах),
- Знать с кем общается подросток в социальных сетях.

Но так же есть правила, которые обязан соблюдать и сам несовершеннолетний, чтобы максимально безопасно проводить время в сети Интернет:

- Не переходить по неизвестным ссылкам,
- Использовать сложные надежные пароли,
- Не посещать сомнительные сайты.

В социальных сетях:

- Использовать двухфакторную аутентификацию,
- Не указывать геолокацию,
- Сделать профиль закрытым,
- Не распространять личную информацию.