Тема 7. Контентные риски. Настройка и безопасное использование смартфона или планшета. Семейный доступ.

Контентные риски — это материалы (тексты, картинки, аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие насилие, агрессию, эротику и порнографию, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду анорексии и булимии, суицида, азартных игр, наркотических веществ и т.д. Столкнуться с ними можно практически везде. Это и сайты, и социальные сети, и блоги, и торренты, и видеохостинги, фактически все, что сейчас существует в Интернете. Зачастую подобный материал может прийти от незнакомца по почте в виде спама или сообщения.

Поиск информации в Сети может быть сопряжен с риском для безопасности компьютера и привести к печальным последствиям для его владельца. В общей массе ссылок, которые появляются в окне браузера в ответ на поисковый запрос, часто оказываются подозрительные ресурсы и фишинговые сайты.

- В первую очередь под прицелом киберпреступников оказываются любители бесплатного и пиратского софта.
- На втором месте по степени опасности находятся запросы информации «для взрослых», которая традиционно используется злоумышленниками для распространения зловредов.
- опасными являются ссылки на сайты с кулинарными рецептами, толкованиями сновидений, советами по уходу за собой и т.п. В подобных случаях злоумышленники пользуются невысоким уровнем знаний по информационной безопасности интернет-пользователей, которые, как правило, интересуются этими темами.
- Не обошли вниманием киберпреступники и всевозможные социальные сети, популярность которых сегодня стремительно растет.
- поиск легкого заработка в Интернете — почти каждая десятая полученная ссылка (9%) грозит заражением компьютера пользователя.

Негативные контентые материалы можно условно разделить на:

- **Незаконные**, к которым могут относиться: детская порнография (включая изготовление, распространение и хранение); наркотические средства (изготовление, продажа, пропаганда употребления), все материалы, имеющие отношение к расовой или религиозной ненависти (экстремизм, терроризм, национализма и др.), а также ненависти или агрессивного поведения по отношению к группе людей, отдельной личности или

животным), азартные игры и т.д.

Внутреннее законодательство каждой страны предусматривает различные виды наказания за распространение такой информации. В Российском законодательстве есть возможность в соответствии со статьями Уголовного кодекса РФ привлечь к административной и уголовной ответственности за распространение подобного негативного контента владельцев сайтов, а также авторов таких электронных текстов и видеопродукции.

- **Неэтичные**, противоречащие принятым в обществе нормам морали и социальным нормам.

Подобные материалы не попадают под действие уголовного кодекса, однако могут оказывать негативное влияние на психику столкнувшимися с ними человека, особенно ребенка. Примерами таких материалов могут служить широко распространенные в сети изображения сексуального характера, в том числе и порнография, агрессивные онлайн игры, азартные игры, пропаганда нездорового образа жизни (употребление наркотиков, алкоголя, табака, анорексии, булимии), принесения вреда здоровью и жизни (различных способов самоубийства, аудионаркотиков, курительных смесей), нецензурная брань, оскорбления, и др. Информация, относящаяся к категории неэтичной может быть также направлена на манипулирование сознанием и действиями различных групп людей.

- **Контентные риски** связаны с другими типами рисков Сети. Например, просмотр тех или иных видео-материалов может привести к заражению компьютера вирусами и потере важных данных. Очень многие распространители подобного негативного контента преследуют цель заразить компьютер, чтобы в дальнейшем иметь возможность манипулировать данными и действиями зараженного компьютера. Пропаганда негативных материалов также может идти через социальные сети, блоги, различные форумы. В данном случае контентные риски пересекаются с коммуникационными.

По данным исследования «Лаборатории Касперского», практически у половины детей в возрасте 4-6 лет уже есть собственный смартфон. Если вы собрались в ближайшее время покупать своему ребенку его первый гаджет или хотите знать больше о том, как сделать работу с устройством безопасной и комфортной, уделите время базовым настройкам смартфона. Для этого стоит учесть ряд особенностей самого устройства, а также возможности специализированного программного обеспечения.

1. Настройки доступа к телефону.

Установка пин-кода или функции TouchID (или FaceID) в самом начале работы со смартфоном позволит сохранить данные на телефоне (фотографии, видео, переписка в

мессенджерах и др.) в случае его потери. Расскажите своему ребёнку о выборе паролей для аккаунтов от различных сервисов. В этом вам поможет наша статья.

Отключите весь функционал, который доступен по отпечатку пальца (TouchID или FaceID), кроме разблокировки телефона, чтобы исключить возможные несогласованные покупки через смартфон или самостоятельную установку приложений. Найти эти функции можно в разделе Настройки — > TouchID (FaceID) и пин-код (для iOS) или Настройки — > Биометрия и безопасность (для Android).

2. Настройка экранного времени.

«Экранное время» — функция, позволяющая фиксировать временной промежуток, который ваш ребенок проводит за гаджетом. Настройка также показывает, какие приложения были задействованы. На основании этих данных программа формирует статистику за день и за неделю.

Найти функцию можно в Настройках –> Экранное время (для iOs) и Настройки -> Использование устройства (для Android).

Кроме того, есть возможность настроить время работы таким образом, что ребенок может «тратить» на социальные сети не больше 3 часов (количество часов можно выбрать произвольное) в день, а также отключить всплывающие уведомления в ночное время. При этом сохраняется возможность настроить исключения для приложений, которые будут вам необходимы.

Функция экранного времени помогает родителям контролировать время, проведенное за экраном смартфона, а детям – избежать переутомления от долгого «общения» с гаджетом.

3. Установка приложений и встроенные покупки.

В самом начале использования смартфона лучше сразу договориться о том, что вы ставите все приложения вместе со своим ребенком. Если вы не знаете, какой контент подходит вашему ребенку, выбирайте категорию для детей в AppStore или GooglePlay.

Приложения в этом разделе уже отобраны согласно интересам ребёнка и возрастным ограничениям.

Для того, чтобы скачать и установить приложение, в зависимости от операционной системы, используйте официальные магазины AppStore или Google Play. Старайтесь избегать установки приложений из ненадёжных источников, чтобы избежать попадания на ваш телефон вирусов и другого зловредного ПО.

Мы всегда можем определить, какое приложение устанавливаем, платное или бесплатное, но практически никогда не обращаем внимание на то, что даже бесплатное

приложение может содержать встроенные покупки. Речь идет о покупках внутри мобильных игр или о платных подписках на различные сервисы. Такая модель получает все большее распространение из-за того, что, с точки зрения коммерческой прибыли, она оказывается более выгодной для производителей программного обеспечения.

В настройках устройства ребёнка (Настройки -> Экранное время -> Контент и конфиденциальность) установите запрет на дополнительные покупки, в том числе опцию запрета на встроенные покупки. Это позволит вам избежать незапланированных расходов, а ребёнку – научиться планировать бюджет.

4. Семейный доступ.

Семейный доступ позволяет всем членам семьи совместно пользоваться приложениями, совершать покупки, создавать общие медиатеки (музыка, видео, книги, документы и др.). Добавлять пользователей может администратор группы, им может стать кто-то из родителей.

По количеству участников в вашей группе может быть для iOS (6 человек) и Android (5 человек). Настройки доступа к семейной группе практически не отличаются для разных операционных систем и не являются сложными, но при этом существенно помогают контролировать расходы и управлять подписками (например, музыка или видеофильмы).

Кроме базовых настроек смартфона, можно воспользоваться специальными приложениями для того, чтобы сделать взаимодействие ребёнка со смартфоном безопасным и удобным Такой программой является Kaspersky Safe Kids, с её помощью можно дополнить базовые настройки телефона, планшета или ноутбука, добавив к ним следующие возможности:

1. Удаленно контролировать использование устройства ребенком.

Доступ к управлению осуществляется через портал https://my.kaspersky.com

2. С помощью функционала Kaspersky Safe Kids вы можете:

- контролировать время работы устройства и установленных приложений;
- устанавливать ограничения по времени работы отдельно взятых приложений;
- смотреть, какие ресурсы часто посещает ваш ребенок.

3. Доступ к геопозиции. Вы всегда будете знать, где находится ваш ребенок.

В данном случае есть возможность включить «безопасный периметр»: функция, которая оповестит вас о том, что ребенок покинул безопасную зону (например, территорию школы или двора).

4. Получать информацию о группах социальной сети, о друзьях, которые к нему добавляются, и о людях, с которыми переписывается ваш ребёнок.

5. Получить консультации детского психолога.

6. Быть в курсе интересов ребёнка и использовать эти знания для выстраивания доверительных отношений с ребёнком.

Важно не только применять технические решения для безопасной работы вашего ребенка в сети Интернет, но и разговаривать с ним о том, что его интересует и что волнует. Любые установленные программы могут вам помочь оградить ребенка от нежелательного контента, и они будут более эффективными, если вы будете знать, как вести себя в разных ситуациях.