***Интернет*** – это объединенные между собой компьютерные сети, глобальная мировая система передачи информации с помощью информационно-вычислительных ресурсов.

По последним данным, в России средний возраст начала самостоятельной работы в Сети - 10 лет, и сегодня наблюдается тенденция к снижению возраста до 6 лет. 30% несовершеннолетних проводят в Сети более 3 часов в день (при норме 2 часа в неделю!). Популярны следующие виды и формы онлайн-развлечений: *социальные сети; сетевые игры; просмотр и скачивание фильмов, клипов, аудиофайлов, программ; обмен файлами; использование электронной почты, сервисов мгновенного обмена сообщениями, чатов; ведение блогов и пр.*

Опасности, с которыми дети могут столкнуться в Сети:

* ***Контакты с незнакомыми людьми с помощью чатов или электронной почты.*** Все чаще и чаще злоумышленники используют эти каналы для того, чтобы заставить детей выдать личную информацию. В других случаях это могут быть педофилы, которые ищут новые жертвы. Выдавая себя за сверстника жертвы, они могут выведывать личную информацию и искать личной встречи.
* ***Неконтролируемые покупки.*** Не смотря на то, что покупки через Интернет пока еще являются экзотикой для большинства из нас, однако недалек тот час, когда эта угроза может стать весьма актуальной. Если Ваши дети имеют доступ к Вашим банковским данным или номеру кредитной карты, они могут приобрести практически что угодно через Интернет, от постера до роскошной машины, или оплатить услуги, варьирующиеся от онлайновых игр до путешествия вокруг света.
* ***Угроза заражения вредоносным ПО.*** Для распространения вредоносного ПО и проникновения в компьютеры используется целый спектр методов. Среди таких методов можно отметить не только почту, компакт-диски, дискеты и прочие сменные носители информации или скачанные из Интернет файлы. Например, программное обеспечение для мгновенного обмена сообщениями сегодня являются простым способом распространения вирусов, так как очень часто используются для прямой передачи файлов. Дети, неискушенные в вопросах социальной инженерии, могут легко попасться на уговоры злоумышленника. Этот метод часто используется хакерами для распространения троянских вирусов. Множество вебсайтов, электронных сообщений или программ обмена файлами позволяют пользователям скачивать все виды музыки, игр, документов и т.д. Однако, несмотря на их кажущуюся безобидность, многие из них содержат вирусы.
* ***Доступ к неподходящей информации:*** сайты, посвященные продаже контрабандных товаров или другой незаконной деятельности; сайты, размещающие изображения порнографического или иного неприемлемого контента, к которым дети могут легко получить доступ; сайты с рекламой табака и алкоголя и т.д. Любопытная детская природа может завести их на сайты расистского, дискриминационного, сексуального, насильственного содержания или на сайты, содержащие материалы, побуждающие ребенка к действиям, которые могут поставить под угрозу его психологическое или физическое здоровье.

**Тревожная статистика:** - 44% детей подвергались домогательствам в Интернете; - 28% детей посещают порнографические веб-страницы; - 50% детей выходят в Интернет одни.

*Компьютерный вирус* — разновидность компьютерных программ или вредоносный код, отличительной особенностью которых является способность к размножению (саморепликация). Как правило, целью вируса является нарушение работы программно-аппаратных комплексов: удаление файлов, приведение в негодность структур размещения данных, блокирование работы пользователей или же приведение в негодность аппаратных комплексов компьютера и т. п. Даже если автор вируса не запрограммировал вредоносных эффектов, вирус может приводить к сбоям компьютера из-за ошибок, неучтённых тонкостей взаимодействия с операционной системой и другими программами. Кроме того, вирусы, как правило, занимают место на накопителях информации и потребляют некоторые другие ресурсы системы.

Создание и распространение вредоносных программ (в том числе вирусов) преследуется в России согласно **Уголовному кодексу РФ (глава 28, статья 273)**. Существует Доктрина информационной безопасности РФ, согласно которой в России должен проводиться правовой ликбез в школах и вузах при обучении информатике и компьютерной грамотности по вопросам защиты информации в ЭВМ, борьбы с компьютерными вирусами, сайтами, не соответствующими задачам образования и обеспечению информационной безопасности в сетях ЭВМ.

*Спам* – это анонимные массовые рассылки электронных писем на электронную почту пользователя, который не давал согласие не ее получения.

Борьба с сетевыми угрозами:

* **Установите комплексную систему защиты!** Установка обычного антивируса – вчерашний день. Сегодня актуальны так называемые «комплексные системы защиты», включающие в себя антивирус, файрволл, антиспам – фильтр и еще пару – тройку модулей для полной защиты вашего компьютера. Новые вирусы появляются ежедневно, поэтому не забывайте регулярно обновлять базы сигнатур, лучше всего настроить программу на автоматическое обновление.
* **Пользуйтесь браузерами Mozilla Firefox, Google Chrome и Apple Safari!** Большинство червей и вредоносных скриптов ориентированы под Internet Explorer и Opera. IE до сих пор удерживает первую строчку в рейтинге популярности, но лишь потому, что он встроен в Windows. Opera очень популярна в России из-за ее призрачного удобства и реально большого числа настроек. Уровень безопасности сильно хромает как у одного, так и у второго браузера, поэтому лучше им и не пользоваться вовсе.
* **Постоянно обновляйте операционную систему!** Эти обновления могут предотвратить вирусные и другие атаки на компьютер, закрывая потенциально опасные точки входа.
* **Будьте осторожны
 с электронной почтой!**Не стоит передавать какую-либо важную информацию через электронную почту. Установите запрет открытия вложений электронной почты, поскольку многие вирусы содержатся во вложениях и начинают распространяться сразу после открытия вложения.
* **Не отправляйте
 SMS-сообщения!** Сейчас очень популярны сайты, предлагающие доступ к чужим SMS и распечаткам звонков, также очень часто при скачивании файлов вам предлагают ввести свой номер, или внезапно появляется блокирующее окно, которое якобы можно убрать с помощью отправки SMS. При отправке SMS, в лучшем случае, можно лишиться 300-600 рублей на счету телефона – если нужно будет отправить сообщение на короткий номер для оплаты, в худшем – на компьютере появится ужасный вирус. Поэтому никогда не отправляйте SMS-сообщения и не вводите свой номер телефона на сомнительных сайтах при регистрации.
* **Используйте сложные пароли!** Как утверждает статистика, 80% всех паролей — это простые слова: имена, марки телефона или машины, имя кошки или собаки, а также пароли вроде 123. Такие пароли сильно облегчают работу взломщикам. В идеале пароли должны состоять минимум из семи, а лучше двенадцати символов. Время на подбор пароля из пяти символов — 2-4 часа, но чтобы взломать семисимвольный пароль, потребуется 2-4 года. Лучше использовать пароли, комбинирующие буквы разных регистров, цифры и разные значки.
* **Делайте резервные копии!** При малейшей угрозе ценная информация с вашего компьютера может быть удалена, а что ещё хуже – похищена. Возьмите за правило обязательное создание резервных копий важных данных на внешнем устройстве –флеш-карте, оптическом диске, переносном жестком диске.
* **Функция «Родительский контроль»
 обезопасит вас!** Для детской психики Интернет – это постоянная угроза получения психологической травмы и риск оказаться жертвой преступников. Не стремитесь утаивать от родителей круг тем, которые вы обсуждает в сети, и новых Интернет-знакомых, это поможет вам реально оценивать информацию, которую вы видите в сети и не стать жертвой обмана.
* **Помните! В Интернете не вся
информация надежна и не все
пользователи откровенны.** Думайте о том, с кем разговариваете. Никогда не разглашайте в Интернете личную информацию, за исключением людей, которым вы доверяете. При запросе предоставления личной информации на веб-сайте всегда просматривайте разделы «Условия использования» или «Политика защиты конфиденциальной информации», чтобы убедиться в предоставлении оператором веб-сайта сведений о целях использования получаемой информации и ее передаче другим лицам. Всегда удостоверяйтесь в том, что вам известно, кому предоставляется информация, и вы понимаете, в каких целях она будет использоваться.