Памятка
по информационной безопасности в сети Интернет

Данный материал подготовлен с целью принятия дополнительных профилактических мер по формированию информационной безопасности в сети Интернет среди учащихся.
Интернет – это не только самая богатая в мире библиотека знаний, развлечений, общения и других полезных вещей, но и источник угроз, представляющих опасность для жизни, физического, психического, нравственного здоровья и полноценного развития ребенка. Необходимо научиться правильно пользоваться этим неисчерпаемым источником информации.

Опасные факторы (угрозы) при работе с компьютером и в сети Интернет:

1. Вредоносные программы, файлы, спамы.
2. Интернет-зависимость.
3. Социальные сети и блоги
4. Кибермошенничество
5. Кибербуллинг
6. Груминг

1. ВРЕДОНОСНЫЕ ПРОГРАММЫ — различное программное обеспечение (вирусы, черви, «троянские кони», шпионские программы, боты и др.), которое может нанести вред компьютеру и хранящимся на нем данным. Они также могут снижать скорость обмена данными с интернетом и даже использовать ваш компьютер для распространения своих копий на другие компьютеры, рассылать от вашего имени спам с адреса электронной почты или профиля какой-либо социальной сети.

Как не подцепить вирус

1) Не открывай материал, присланный незнакомцами.
2) Не открывай сомнительный файл с вложениями, даже если ты получил его от своего знакомого. Свяжись с другом, от которого ты получил сообщение, и уточни у него, действительно ли он является автором послания
3) Не запускай и не скачивай файлы (например, музыку, фильмы, игры) из сомнительных источников.
4) Старайся не нажимать на рекламные баннеры, даже если они кажутся тебе очень заманчивыми.
5) Старайся не посещать сомнительные сайты или ресурсы.
6) Для защиты от спама:
не выдавай в Интернет своего реального электронного адреса, есть риск использования твоего почтового ящика в качестве рассылки спама;
старайся чаще менять пароли к электронной почте, к страничке в социальной сети и др.
7) Заведи себе два адреса — частный, для переписки (приватный и малоизвестный, который ты никогда не публикуешь в общедоступных источниках), и публичный — для публичной деятельности (форумов, чатов и так далее).
8) Если ты не пользуешься компьютером, старайся отключать его от соединения с Интернетом.

Борьба с вирусами

1) Не сохраняй на своем компьютере неизвестные файлы. Подозрительные сообщения лучше немедленно удалять:
удали сообщение из папки Входящие;
удали сообщение из папки Удаленные (Корзина);
выполни над папками операцию "Сжать" (Файл/Папка/Сжать все папки).

Если твой компьютер заражен:
Отключи компьютер от Интернета и локальной сети.
Не пытайся самостоятельно решить проблему, не жми на все кнопки подряд, посоветуйся со взрослым.
Или, если необходимо, то обратись за помощью в службу технической поддержки производителя установленного на твоем компьютере антивирусного ПО.

Если ты уверенный пользователь компьютера:
Загрузи компьютер в безопасном режиме (включи компьютер, нажми и, удерживая клавишу F8, выбери Безопасный режим (Safe Mode) в открывшемся меню).
Проведи полную антивирусную проверку компьютера.
Если в результате проверки обнаружен вирус, червь или троянская программа, следуйте указаниям производителя антивирусного ПО. Хорошие антивирусы предлагают лечение зараженных объектов, помещение подозрительных объектов в карантин и удаление троянских программ и червей.

2. ИНТЕРНЕТ - ЗАВИСИМОСТЬ среди подростков, которая появляется в навязчивом желании неограниченно долго продолжать сетевое общение, появляется склонность к эмоциональному возбуждению, агрессии, неконтролируемым действиям.
3. СОЦИАЛЬНЫЕ СЕТИ и БЛОГИ, на которых ребенок оставляет о себе немало настоящей информации, завязывает небезопасные знакомства, нередко подвергается незаметной для него психологической и нравственно-духовной атаке. Злоумышленникам особенно легко искать своих несовершеннолетних жертв с помощью таких сайтов как «В контакте», «Одноклассники» и «Мой мир».
6. КИБЕРМОШЕННИЧЕСТВО — один из видов киберпреступления, целью которого является обман пользователей, например, хакер незаконно получает доступ к личной информации пользователя (номера банковских счетов, паспортные данные, коды, пароли и др.) с целью причинить материальный или иной ущерб. Отправка любых SMS на короткие номера сотовых операторов с последующим списанием средств со счета мобильного телефона сверх указанной ранее суммы либо без получения указанной услуги также является видом кибермошенничества.

Предупреждение кибермошенничества

1) Ни под каким предлогом не выдавай незнакомым людям свои личные данные (домашний адрес, номер телефона и т.д.) и пароли.
2) Перед тем, как воспользоваться развлекательными услугами Интернета (скачать музыку, фильм и т.д.), проверь, что после этого тебя не попросят заплатить деньги.
3) Не верь всему, что видишь в Интернет.
4) Старайся остерегаться новых предложений и услуг, все они требуют вложения крупной суммы денег (например, местонахождение человека по номеру его мобильного, повышение рейтинга в социальной сети и т.д.)
5) Советуйся со взрослыми перед тем, как загрузить, скачать или установить ту или иную услугу.
6) Очень внимательно выбирай сайты, на которых ты хочешь сделать покупки и удостоверься в их надежности. Собери как можно больше информации о сайте, спросив, например, название, адрес и номер телефона центрального офиса, описания общих положений контракта и, особенно о том, как отменить заказ; кроме того выясни о защите и управлении личными данными и безопасности оплаты; и сравни цены, отыскав такой же предмет на других сайтах.

7) Если ты получил неожиданное электронное письмо, в котором тебе предлагается невероятно выгодная сделка, вероятность того, что это мошенничество, очень велика.

Борьба с кибермошенничеством

1) Если компьютер подцепил вирус, не отправляй смс сообщение, даже если тебе обещают таким образом очистить компьютер от вредоносных программ или разблокировать компьютер.

2) В случае взлома страницы в социальной сети — смени пароли.

3) Обратись за советом к взрослому.

5. КИБЕРБУЛЛИНГ (cyberbullying) — преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных Интернет-сервисов: электронную почту, сервисы мгновенных сообщений, в чатах, социальных сетях, на web-сайтах, а также посредством мобильной связи. Наиболее опасные виды **кибербуллинга:**

Киберпреследование – скрытое выслеживание жертвы с целью организации нападения, избиения, насильственных действивй и т.д.;

Хеппислепинг (Happy Slapping) – видеоролики с записями реальных сцен насилия; Б**уллицид** – доведение ребенка до самоубийства путем психологического воздействия; **Груминг –** наиболее опасный вид (см.ниже).

Предупреждение кибербуллинга

1) Не сообщай свои данные агрессору (реальное имя, фамилию, адрес, телефон, номер школы и т.п.). Когда злоумышленнику становятся известны твои анкетные данные, происходит так называемый «троллинг» или травля.

2) Не открывай доступ к своей страничке незнакомым людям.

3) Следи за информацией, которую ты выкладываешь в Интернете

4) Придерживайся правил сетевой этики, не отвечай грубо на сообщения, этим ты можешь спровоцировать собеседника. Игнорируй сообщения от незнакомых, агрессивных и подозрительных личностей. Нужно понимать, что онлайн-общение не является приватным. Другие пользователи могут скопировать, распечатать или переслать твою личную переписку.

5) Если ты видишь или знаешь, что твоего друга запугивают, поддержи его и сообщи об этом.

6) Не посылай сообщения или изображения, которые могут огорчить кого-нибудь.

Борьба с кибербуллингом

1) Не предпринимай самостоятельных действий по наказанию агрессора

2) Немедленно обратись за советом к родителям или в специальные организации за помощью

3) Сделай снимок экрана с оскорблениями (screen-shot) и перешлите его модераторам ресурса.

4) Или напиши письмо в техподдержку с просьбой удалить аккаунт хулигана. Важно помнить, что адекватно отреагировав на неприятное сообщение, оповестив администрацию ресурса о киберхулигане, можно обезопасить от него, не только себя, но и остальных пользователей.

5) Если же преследование происходит лично, с помощью электронной почты, сервисов мгновенных сообщений (ICQ, Google talk и т.д.) или IP телефонии (Skype) избавиться от неприятного собеседника можно нажав клавишу «игнорировать» (или «черный список»). У большинства программ, предназначенных для общения, существует такая или аналогичная функция.

6. ГРУМИНГ — 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 (адрес, телефон и др.) и договориться о встрече.

Предупреждение груминга

1) Следи за информацией, которую ты выкладываешь в Интернете. Не выкладывай свои личные данные в Интернете (домашний адрес, номер телефона, номер школы, класс, любимое место прогулки, время возвращения домой, место работы отца или матери и т.д.). Помни, любая информация может быть использована против тебя, в том числе в корыстных и преступных целях

2) Используй псевдоним при общении в чатах, использовании программ мгновенного обмена сообщениями (типа ICQ, Microsoft Messenger и т.д.), пользовании он-лайн играми и других ситуациях

3) Не размещай и не посылай свои фотографии незнакомцам

4) Будь осторожен при общении с незнакомыми людьми. Старайся рассказывать как можно меньше информации о себе.

Борьба с грумингом

1) Если новый знакомый пытается говорить с тобой на неприятные или пугающие тебя темы и говорит об этом как о секрете, который останется только между вами – немедленно сообщи об этом родителям или старшим

2) Сделай снимок с экрана (screen-shot)

3) Никогда не соглашайся на личные встречи с незнакомцами. Твои собеседники могут оказаться совсем не теми, за кого себя выдают. Или приходи на встречу только со взрослым.

Памятка
по информационной безопасности для учащихся

Раздел 1. Интернет

Надо мной издеваются в Интернете…

Первое, что необходимо предпринять – это собрать доказательства издевательств над тобой. Потом отправь жалобу администраторам данного ресурса с просьбой принять меры против обидчика. Второе, заблокируй отправку сообщений от обидчика. И третье, прояви выдержку и не ввязывайся в конфликт.

Кто-то в сети разместил фотографию/ видео со мной без моего разрешения…

Обратись к человеку, который непосредственно разместил у себя твою фотографию. Попроси его удалить эту фотографию. Если же человек отказывается, то обратись к администраторам ресурса, на котором была размещена твоя фотография. Если же и администраторы откажут, то необходимо обратиться в суд, но это ты уже должен сделать вместе с родителями. Расскажи о данном факте учителю, классному руководителю, завучу в школе.

На многих сайтах теперь можно зайти через аккаунт в социальной сети. Безопасно ли это?

Да, это безопасно. Если ты хочешь авторизоваться через какую-то социальную сеть, то должно появиться окно браузера, где будет открыт сайт этой социальной сети и у тебя уточнят, хочешь ли ты предоставить этому сайту доступ к твоему аккаунту. Если все эти условия будут выполнены, то твоя сессия от имени твоего аккаунта будет безопасна.

Какой пароль является безопасным?

Восемь или не менее 8 символов в длину и содержать комбинацию букв, цифр и символов. Вот пример сложного пароля: $tR0ng!Ты можешь оценить свой пароль на разных ресурсах, которые проверяют надежность паролей.

На мой мобильный телефон пришла смс от администрации социальной сети, где я зарегистрирован. Они просят в рамках проверки достоверности аккаунта выслать свой логин и пароль. Должен ли я отправлять им свои данные?

Нет. Скорее всего, это мошенники, которые хотят получить доступ к твоему аккаунту. Тебе необходимо уведомить техподдержку социальной сети о случае фишинга.

Где я могу скачать игру бесплатно и без вирусов?

Есть несколько вариантов. Можно использовать игры, которые раздаются бесплатно, и скачивать их лучше с официального сайта игры, сайта разработчика или его официального партнера. Во всех остальных случаях никаких гарантий безопасности нет.

Мой аккаунт взломали в социальной сети. Что мне делать?

Отправь администраторам ресурса письмо, где сообщи о том, что твой аккаунт взломали и попроси заблокировать его. Также необходимо предупредить всех друзей, которые у тебя добавлены в сети, о том, что тебя взломали и от твоего имени могут приходить сообщения. Проверь компьютер на наличие вирусов. Полезной мерой также может стать смена паролей на других сервисах и сайтах, так как злоумышленники, получив один пароль, могут получить доступ к твоим аккаунтам на других сайтах.

В адресной строке появляется значок ключа. Что он означает?

Это означает, что браузер установил безопасное соединение с просматриваемым веб-сайтом. Это происходит, когда ты набираешь конфиденциальную информацию типа «Логин» и «Пароль».

В игре у меня не сложились отношения с человеком, и он меня преследует. Что мне делать?

Заблокируй его в списках своих друзей, подобная функция есть во многих онлайн играх. Если это приложение в социальной сети, то блокировка недругов осуществляется через блокировку профиля. Также можно пожаловаться администраторам игры на этого человека, но необходимо

будет предъявить доказательства. Если он угрожает тебе расправой, сообщи родителям, учителю или завучу школы.

Я познакомился с человеком в сети, и он склоняет меня к противоправным или непорядочным действиям…

Эта ситуация опасна, поэтому сообщи об этом своим родителям и обратись с ними в полицию.

Мой компьютер повис, когда я зашел на какой-то сайт. Что мне делать?

Используй комбинацию клавиш ctrl-alt-delete или ctrl-shift-esc, закрой браузер, где был открыт этот сайт.

Что такое файлы Cookie и надо ли их удалять?

Файлы Cookie– это маленькие текстовые файлы, которые содержат логин и пароль пользователя для доступа к каком-то сайту. Таким образом, человек, который возвращается на этот сайт, входит без авторизации. Большинство файлов Cookie создается сайтами, которые посещает пользователь, и эти файлы предназначены для работы самого сайта.

Однако некоторые файлы Cookie создаются на компьютере без твоего ведома, с целью изучить как и что ты делал на каком-то ресурсе. Также они могут быть использованы и во вред, поэтому ты можешь их удалять. Также это сделает сам браузер, когда ты из него выйдешь.

Раздел 2. Компьютер

Мой компьютер взломали, что делать?

Если есть возможность - запусти антивирусную программу, а в настройках антивирусника установи максимальные требования к проверке компьютера.

Если программа не работает, то лучше переустановить операционную систему компьютера. Или восстановить состояние операционной системы до предыдущей даты. Это можно сделать следующим способом: нажать «Пуск», выбрать в меню «Все программы», найти «Стандартные», открыть «Служебные», и нажать на «Восстановление системы».

У тебя на рабочем столе висит баннер, который предлагает избавиться от него за деньги. Воспользуйся сервисами от разработчиков антивирусов, которые помогут тебе избавиться от баннеров. Вот ссылки на эти сервисы:sms.kaspersky.ru, www.drweb.com/xperf/unlocker/.

Также тебе будет необходимо поменять пароли доступа к твоим профайлам в сети, так как вирус может получить доступ к ним.

Где найти бесплатные антивирусные программы?

Наиболее популярные бесплатные антивирусные программы AviraAntivirPersonal, AVG и Avast.Ты можешь установить одну из этих программ. Рекомендуется использовать также бесплатный сканер от Касперского , либо утилиту drwebcureit или сканер от McAfee для периодической проверки твоего компьютера, поскольку бесплатные антивирусные программы не являются достаточно надежными.

Где потенциально в сети я могу заразить свой компьютер?

Это можно сделать практически везде, даже на крупных сайтах, правда, вероятность заражения на этих сайтах меньше. Источником вирусов может быть система файлообмена, сайт по приготовлению еды, электронная почта, чат и т.п. Некоторые поисковые системы отслеживают, является ли сайт безопасным или нет.

Что такое брандмауэр и работает ли он на моем компьютере?

Брандмауэр - это бесплатная программа, которая проверяет данные, входящие через Интернет, блокирует их или позволяет им поступить в компьютер. По сути, он помогает отражать атаки хакеров, вирусов и червей, пытающихся попасть на компьютер через Интернет. Брандмауэр предустановлен во всех версиях операционной системы выше Windows XP, но возможно, он отключен. Проверить это можно следующим образом: нажать кнопку «Пуск», выбрать «Панель управления», потом «Брандмауэр».

Раздел 3. Электронная почта

Нужно ли отвечать на сообщение со спамом?

Этого не стоит делать, т.к. спамеры могут узнать о том, что твой email действующий, и могут дальше отсылать тебе спам.

Прислали письмо с файлом, отправителя не знаю. Что делать?

Скорее всего, этот файл с вирусом. Чтобы знать точно, запусти проверку этого файла антивирусной программой. Но лучше сообщение удалить, не открывая его.

Пришло письмо с файлом от знакомого отправителя, но я не ждал этого файла. Можно ли открывать файлы от знакомых отправителей?

Не исключено, что электронная почта твоего знакомого взломана и в этом сообщении находится вирус. Если отправитель тебя не уведомлял, что планирует отправлять файлы, то лучше позвонить ему или отправить запрос по электронной почте либо в социальной сети, уточнив от него ли это сообщение.

Какой лучше выбрать адрес электронной почты?

Лучше выбрать тот адрес электронной почты, который не содержит никаких личных сведений. Например, лучше выбрать «музыкальный_фанат@» или «рок2013» вместо «петя13».

Раздел 4. Мобильная связь

Мне приходят СМС с оскорблениями, унижающими текстами…

Об этом нужно проинформировать родителей и вместе с ними обратиться к оператору сотовой связи с просьбой выяснить, кто это делает, и заблокировать его. Если же обидчик будет продолжать свои действия, то необходимо обратиться в полицию.

Могут ли посторонние подключаться к моему Bluetooth и является ли это угрозой?

Bluetooth является угрозой в том случае, когда он открыт и на нем нет пароля доступа. Люди в зоне действия Bluetooth могут получить доступ к файлам в твоем телефоне и твои контакты.

Украли мобильный телефон. Что мне делать?

Первое – проинформируй родителей о случившемся, потом обратись к оператору сотовой связи и попроси заблокировать сим-карту, таким образом ты сохранишь свои деньги. Также необходимо предупредить всех знакомых, которые у тебя были добавлены в телефонную книгу, о том, что у тебя украли телефон, и возможно им будет идти спам от твоего имени.

Купив новый телефон и восстанавливая телефонные контакты, скопируй их на компьютер или перепиши в записную книжку.