Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Кубанский государственный технологический университет»

Актуальные угрозы информационной безопасности подростков и молодёжи

Краснодар 2019

Цель

обучение информационной безопасности молодёжи и подростков путем привития навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде.

Содержание

Информационная безопасность

Опасность - это возможность нанесения вреда, имущественного (материального), физического или морального (духовного) ущерба личности, обществу государству

Информационная безопасность - состояние сохранности информационных ресурсов и защищенности законных прав личности и общества в информационной сфере, процесс обеспечения конфиденциальности, целостности и доступности информации

Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями и дополнениями)

Система ГАРАНТ: http://base.garant.ru/12148555/#ixzz3SCxX7hvZ

Основные принципы

Конфиденциальность	• Обеспечение доступа к информации только авторизованным пользователям
Целостность	• Обеспечение достоверности и полноты информации и методов ее обработки
Доступность	• Обеспечение доступа к информации авторизованным пользователям по мере необходимости

Что такое Интернет

Интернет открыл для человека новые, безграничные возможности общения, именно Интернет стирает все границы, обеспечивая распространение любой информации для неограниченного круга людей

Главное назначение Интернет - это свободный доступ, распространение информации и установление связи между всеми людьми планеты

Проблемы Интернет

- Интернет - это публичная открытая сеть с нецентрализованными топологией и маршрутизацией
- Вредоносная активность может возникнуть в одной части Интернета и затем быстро распространиться по всей Всемирной сети
- В Интернете контролируется главным образом, входящий трафик, но не исходящий
- Во Всемирной сети практически отсутствует идентификация пользователей
- Юрисдикция страны, в которой произошло преступление, зачастую не распространяется на киберпреступника

Актуальные угрозы Интернет

- Кража данных в результате атак на мобильные устройства
- Заражение вредоносными программами и разглашение конфиденциальной информации в социальных сетях
- Незаметное инфицирование компьютеров и других устройств при посещении безопасных на первых взгляд веб-сайтов
- Использование недостаточно защищенных облачных веб-сервисов и технологии

Последствия

1) Утечка персональных данных
2) Утечка переписки, личных фотографий
3) Искажение информации
4) Интернет-зависимость
5) Заражению вредоносными программами при скачивании файлов
6) Нарушению нормального развития.
7) Неправильное формирование нравственных ценностей.
6) Знакомство с человеком с недобрыми намерениями.

Нормативно-правовые акты

В Российской Федерации к нормативно-правовым актам в области информационной безопасности относятся:

- Конституция РФ
- Законы федерального уровня (включая федеральные конституционные законы, кодексы)

Федеральный закон № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию“

УК РФ Статья 137. Нарушение неприкосновенности частной жизни

- Указы Президента РФ
- Постановления Правительства РФ
- Нормативные правовые акты федеральных министерств и ведомств
- Нормативные правовые акты субъектов РФ, органов местного самоуправления и т. д.

Международные нормы и нормативные правовые акты РФ, регулирующие вопросы информационной безопасности среди подростков и молодёжи

Нормы международного права

1)ст. 13, 17, 34 Конвенции ООН о правах ребенка 1989 г.,
2)Европейской декларацией о свободе обмена информацией в Интернете 2003 г.,
3)Европейской конвенцией о совместном кинопроизводстве 1992 г.,
4)Европейской конвенцией о трансграничном телевидении 1989 г.,
5)Европейской конвенцией о правонарушениях в сфере электронной информации 2001 г;
6)Европейской рамочной конвенцией о безопасном использовании мобильных телефонов маленькими детьми и подростками
7)(06.02.2007);
8)Рекомендациями Комитета Министров государств — членов Совета Европы: № R (89) 7 — относительно принципов
9)распространения видеозаписей, содержащих насилие, жестокость или имеющих порнографическое содержание (22.04.1989),
10)№ R (97) 19 — о демонстрации насилия в электронных средствах массовой информации (30.10.1997),
11)Рекомендация Rec (2001) 8 – в сфере регулирования в отношении кибер-контента (саморегулирования и защиты пользователей
12)от незаконного или вредного содержания новых коммуникаций и информационных услуг),
13)№ Rec (2003) 9 – о мерах поддержки демократического и социального распространения цифрового вещания (28.05.2003),
14)Рекомендации Rec (2006) 12 по расширению возможностей детей в новой информационно-коммуникационной среде (27.09.2006),
15)CM/Rec (2007) 11 о поощрении свободы выражения мнений и информации в новой информационной и коммуникационной среде,
16)CM/Rec (2008) 6 о мерах по развитию уважения к свободе слова и информации в связи с Интернет-фильтрами;
17)Рекомендациями Европейского парламента и Совета ЕС о защите несовершеннолетних и человеческого достоинства и права на
18)ответ в отношении конкурентоспособности индустрии европейских аудиовизуальных и информационных он-лайн услуг
(20.12.2006);
19)Модельным законом МПА СНГ «О противодействии торговле людьми», принятым на тридцатом пленарном заседании
20)Межпарламентской Ассамблеи государств – участников СНГ (03.04.2008);
21)Рекомендациями по унификации и гармонизации законодательства государств — участников СНГ в сфере борьбы с торговлей
22)людьми (03.04.2008);
23)Модельным законом МПА СНГ «О защите детей от информации, причиняющей вред их здоровью и развитию» (03.12.2009);
24)Рекомендациями по унификации и гармонизации законодательства государств — участников СНГ в сфере защиты детей
25)от информации, причиняющей вред их здоровью и развитию (28.10.2010);

Федеральное законодательство

1) ст. 14, 14.1 Федерального закона от 24.07.1998 № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации»,
2) ст. 31 Основ законодательства Российской Федерации о культуре от 09.10.1992 № 3612-1,
3) ст. 4, 37 Закона Российской Федерации от 27.12.1991 «О средствах массовой информации» № 2124-1,
4) ст. 46 Федерального закона от 08.01.1998 № 3-ФЗ «О наркотических средствах и психотропных веществах»,
5) Федеральным законом от 13.03.2006 № 38-ФЗ «О рекламе», Федеральным законом от 29.12.2010 № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию" (вступает в действие 01.09.2012),
6) Федеральный закон от 21.07.2011 № 252-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона "О защите детей от информации, причиняющей вред их здоровью и развитию",
7) Стратегия национальной безопасности Российской Федерации до 2020 года, утвержденной Указом Президента Российской Федерации от 12.05.2009 № 537,
8) Доктрина информационной безопасности Российской Федерации, утвержденной Президентом Российской Федерации 09.09.2000 № ПР-1895, в которых закреплены общие принципы обеспечения информационной безопасности граждан и государства.

Угрозы безопасности подростков в сети Интернет

В виртуальном пространстве сети Интернет существует множество угроз, с которыми практически ежедневно сталкиваются и взрослые пользователи, и дети, и подростки. Все угрозы можно разделить на несколько видов:

1) Угрозы компьютерной технике и программному обеспечению (электронная безопасность)
2) Психологические угрозы
3) Угрозы материального характера (потеря денег),

- ущерб нанесенный физическим лицам, чья информация была похищена

-затраты на восстановление систем информации.

-затраты, связанные с невозможностью выполнения работы из-за перемен в системе защиты информации.

4) Моральные угрозы , связанный с репутацией или повлекший нарушения взаимоотношений

Электронная безопасность

Риски, связанные с электронной безопасностью, относятся к различной кибердеятельности, которая включает в себя: разглашение персональной информации, выход в сеть с домашнего компьютера с низким уровнем защиты (риск подвергнуться вирусной атаке), онлайн-мошенничество и спам.

Вредоносные программы

Вредоносные программы - это программы, негативно воздействующие на работу компьютера.

К ним относятся

1) вирусы,
2) программы-шпионы,
3) нежелательное рекламное программное обеспечение различные формы вредоносных кодов.

Виды вредоносных программ

1. **Компьютерные вирусы**, нарушающие информационную безопасность. Они оказывают воздействие на информационную систему одного компьютера или сети ПК после попадания в программу и самостоятельного размножения. Вирусы способны остановить действие системы, но в основном они действуют локально;
2. **«Черви»** – модификация вирусных программ, приводящая информационную систему в состояние блокировки и перегрузки. ПО активируется и размножается самостоятельно, во время каждой загрузки компьютера. Происходит перегрузка памяти и каналов связи;
3. **«Троянские кони»** – программы, которые внедряются на компьютер под видом полезного обеспечения. Но на самом деле они копируют персональные файлы, передают их злоумышленнику, разрушают полезную информацию.

Угроза заражения вредоносным программным обеспечением

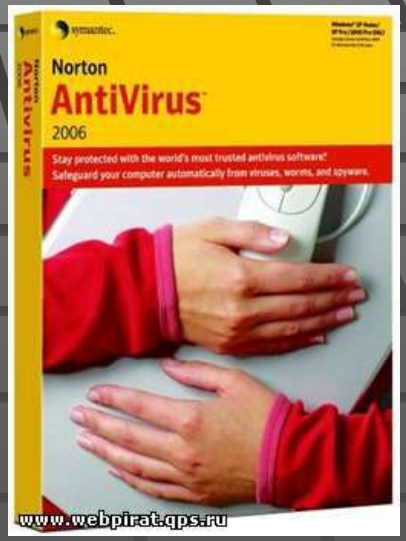
Для распространения вредоносного ПО и проникновения в компьютеры используется целый спектр методов

Места обитания:

- электронная почта;
- телеконференции и электронные доски объявлений в Интернет;
- свободное и условно свободное программное обеспечение в сети Интернет;
- локальные компьютерные сети организаций, создающие удобную среду для заражения вирусами объектов на других рабочих станциях;
- обмен зараженными файлами на различных носителях между пользователями КС;
- использование нелицензионных компакт-дисков.

Защита от заражения

Обязательным средством антивирусной защиты является использование специальных программ для обнаружения и удаления вирусов в различных объектах КС.



Удаление вирусов

При автоматическом удалении обнаруженных антивирусными программами вирусов могут применяться два основных метода:

- удаление уже известных вирусов с помощью заранее разработанного алгоритма лечения;
- попытка удаления неизвестных до этого времени вирусов на основе сведений об общих принципах работы вирусов и (или) предварительно сохраненной информации о незараженном файле.

Рекомендуется перед удалением обнаруженных вирусов выполнить копирование зараженных файлов на резервный носитель информации, чтобы не потерять ценных данных.

Предупреждение столкновения с вредоносными программами:

1) Установите на все домашние компьютеры специальные почтовые фильтры и антивирусные системы для предотвращения заражения программного обеспечения и потери данных. Такие приложения наблюдают за трафиком и могут предотвратить как прямые атаки злоумышленников, так и атаки, использующие вредоносные приложения.
2) Используйте только лицензионные программы и данные, полученные из надежных источников. Чаще всего вирусами бывают заражены пиратские копии программ, особенно игр.
3) Важно использовать только проверенные информационные ресурсы и не скачивать нелицензионный контент.
4) Периодически старайтесь полностью проверять свои домашние компьютеры.
5) Делайте резервную копию важных данных.
6) Старайтесь периодически менять пароли (например, от электронной почты) и не используйте слишком простые пароли.

Будь готов

Сложные разновидности даже известных вирусов не всегда могут быть удалены, а зараженные ими файлы восстановлены. Поэтому для обязательной подготовки к возможному заражению объектов КС вирусами необходимо:

- подготовить защищенный от записи загрузочный диск, записав на него последние версии антивирусных программ и баз сигнатур;
- постоянно обновлять установленное в КС антивирусное ПО;
- регулярно проверять объекты КС всеми имеющимися антивирусными программами);
- обязательно проверять на наличие вирусов все входящие сообщения электронной почты и присоединенные к ним файлы;
- регулярно выполнять резервное копирование наиболее важных системных и прикладных файлов;
- минимизировать число каналов распространения вирусов.

Программы-шпионы

Spyware устанавливается в системе без Вашего согласия.

Основная задача - взять контроль над компьютером и отправить вашу личную информацию третьему лицу.

Ещё одна разновидность шпионских программ - **клавиатурные шпионы**. Эти spyware для получения вашей личной информации используют захват нажатий клавиш.

Признаками заражения ПК шпионскими программами может служить следующее:

1) Изменение стартовой страницы поисковой системы.
2) Всплывающие рекламные окна.
3) Изменение поисковой системы.
4) Не нужные панели инструментов в браузере.
5) Низкая производительность системы.

Программы-шпионы

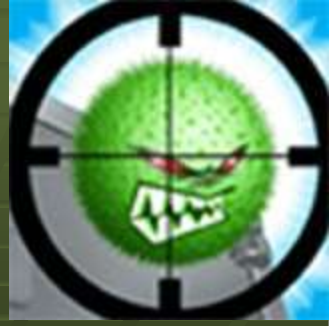
При соблюдении правильной политики безопасности в КС, использующих защищенные версии операционных систем, внедрение в них программных закладок практически невозможно.

Однако соблюдение адекватной угрозам политики безопасности сколько-нибудь продолжительное время также практически невозможно.

Что такое программа-антишпион.

Анти-шпионские программы это отдельные приложения ориентированные конкретно на spyware и adware. Конечно, антивирусные программы обнаруживают некоторые программы-шпионы, но антишпионские программы в этом деле гораздо эффективнее. И хотя производители считают, что для Windows достаточно встроенного Windows Defender. Поставить антишпионскую программу от стороннего производителя совсем не помешает.

Обнаружение закладок



Могут быть разработаны программы для автоматизации действий по обнаружению программных закладок.

В частности, некоторые антивирусные программы могут обнаруживать инсталляторы закладок и сами закладки.

Однако новые разновидности закладок могут преодолевать защиту, обеспечиваемую данными автоматизированными средствами.

Методы защиты

Эффективным методом защиты от вредоносных программ является создание изолированной программной среды, обладающей следующими свойствами:

- исключен запуск любых программ в данной программноаппаратной среде, кроме проверенных;
- исключен запуск проверенных программ вне проверенной среды их выполнения.

Требуется тщательный анализ новой информации о типах вирусов и программных закладок и способах их внедрения в КС для выбора подходящих методов защиты.

Спам

Спам - это нежелательные электронные письма, содержащие рекламные материалы. Спам дорого обходится для получателя, так как пользователь тратит на получение большего количества писем свое время и оплаченный интернет-трафик. Также нежелательная почта может содержать, в виде самозапускающихся вложений, вредоносные программы.

Пять правил безопасного пользования электронной почтой:

1) Никогда не открывайте подозрительные сообщения или вложения электронной почты, полученные от незнакомых людей. Вместо этого сразу удалите их, выбрав команду в меню сообщений.
2) Никогда не отвечайте на спам.
3) Применяйте фильтр спама поставщика услуг Интернета или программы работы с электронной почтой (при наличии подключения к Интернету).
4) Создайте новый или используйте семейный адрес электронной почты для Интернет-запросов, дискуссионных форумов и т.д.
5) Никогда не пересылайте «письма счастья». Вместо этого сразу удаляйте их.

P.S «**Письмо́ сча́стья**» или «магическое письмо» — термин, обозначающий сообщение, нередко религиозно-мистического содержания, рассылаемое по электронной или обычной почте (а также в сетях мгновенного обмена сообщениями и социальных сетях в Интернете) нескольким адресатам с призывом или требованием, чтобы получатель распространил копии сообщения дальше.

Кибермошенничество

Кибермошенничество - это один из видов киберпреступлений, целью которого является обман пользователей. Хищение конфиденциальных данных может привести к тому, что хакер незаконно получает доступ и каким-либо образом использует личную информацию пользователя, с целью получить материальную прибыль. Есть несколько видов кибермошенничества: нигерийские письма, фишинг, вишинг и фарминг.

Кибермошенничество

Фи́шинг (англ. 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, например, от имени банков или внутри социальных сетей. В письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с перенаправлением на сайт хакера. После того как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приёмами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определённому сайту, что позволяет мошенникам получить доступ к пользовательской информации и банковским счетам.

Фишинг — одна из разновидностей социальной инженерии, основанная на незнании пользователями основ сетевой безопасности: в частности, многие не знают простого факта: сервисы не рассылают писем с просьбами сообщить свои учётные данные, пароль и прочее.

Для защиты от фишинга производители основных интернет-браузеров договорились о применении одинаковых способов информирования пользователей о том, что они открыли подозрительный сайт, который может принадлежать мошенникам. Новые версии браузеров уже обладают такой возможностью, которая соответственно именуется «антифишинг».

Кибермошенничество

Вишинг — это один из методов мошенничества с использованием социальной инженерии, который заключается в том, что злоумышленники, используя телефонную коммуникацию и играя определенную роль (сотрудника банка, покупателя и т. д.), под разными предлогами выманивают у держателя платежной карты конфиденциальную информацию или стимулируют к совершению определенных действий со своим карточным счетом / платежной картой.

Фарминг (“farming”) – занятие сельским хозяйством, животноводством). Злоумышленник распространяет на компьютеры пользователей специальные вредоносные программы, которые после запуска на компьютере перенаправляют обращения к заданным сайтам на поддельные сайты. Таким образом, обеспечивается высокая скрытность атаки, а участие пользователя сведено к минимуму – достаточно дождаться, когда пользователь решит посетить интересующие злоумышленника сайты.

Доступ к нежелательному содержимому

Любой подросток, выходящий в сеть Интернет, может просматривать любые нежелательные материалы

К таким материалам относятся:

- страницы с националистической или откровенно фашистской идеологией
- насилие
- наркотики
- Порнография
- многое другое

Полезные советы по работе в сети Интернет

1) Всегда помни свое Интернет-имя (E-mail, логин, пароли) и не регистрируйся везде без надобности.
2) Не поддавайся ярким рекламам-указателям и не ходи на подозрительные сайты.
3) Если пришло письмо о крупном выигрыше - это «обманная почта»: просто так выиграть невозможно.
4) Чтобы вернуться назад и вернуться вовремя, заводи себе будильник, садясь за компьютер.
5) Если хочешь дружить с людьми из других стран, изучай полезные сервисы, блоги, форумы друзей и т.д.
6) Не забывай обновлять антивирусную программу.
7) Не скачивай нелицензионные программные продукты.
8) Номер всероссийского детского телефона доверия

(8-800-2500015)

Другие угрозы

Анорекси́я (др.-греч. α- «без-, не-» + ὄρεξις «позыв к еде») —синдром, заключающийся в полном отсутствии аппетита при объективной потребности организма в питании, который сопровождает большинство метаболических заболеваний, инфекций, болезней пищеварительной системы, в частности паразитарных инфекций, а также возникающий по другим причинам. Анорексия может приводить к смерти.

Булимия - психологическое расстройство, связанное с нарушением пищевого поведения, склонностью реагировать на различные стрессовые ситуации, поглощая чрезмерное количество пищи.

Самоуби́йство, **суици́д** (от лат. *sui caedere* — убивать себя) — преднамеренное лишение себя жизни, как правило, самостоятельное и добровольное.

термин «**груминг**», обозначает 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 и договориться о встрече.

Даже если у большинства пользователей чат-систем (веб-чатов или IRC) добрые намерения, среди них могут быть и злоумышленники. В некоторых случаях они хотят обманом заставить подростков выдать личные данные, такие как домашний адрес, телефон, пароли к персональным страницам в Интернете и др. В других случаях они могут оказаться преступниками в поисках жертвы.

Полезные советы

1) Выбирайте пароль посложнее, состоящий из символов разного регистра, с цифрами и для абсолютной надёжности - знаками препинания.

- Не используйте пароль, связанный с теми данными, которые могут быть о вас известны, например, ваше имя или дату рождения.
- Пароли, которые вы видите на экране создаются в реальном времени на вашем компьютере, поэтому исключена возможность перехвата пароля по сети. Разные посетители сайта видят разные пароли. Если вы зайдете на сайт второй раз, пароли будут другими.
- Вы можете выбрать пункт меню браузера "Файл|Сохранить как...", чтобы пользоваться генератором паролей в оффлайне.
- Генератор паролей полностью прозрачен: скачайте файл passwd.js, чтобы увидеть, как создается пароль, и убедиться в абсолютной надежности.

Источник- http: //genpas. narod. ru/

2) Заходите в интернет с компьютера, на котором установлен фаервол или антивирус с фаерволом. Это в разы уменьшит вероятность поймать вирус или зайти на вредоносный сайт.

3) Заведите один основной почтовый адрес и придумайте к нему сложный пароль. При регистрации на форумах, в соц. сетях и прочих сервисах Вы будете указывать его. Это необходимо если Вы забудете пароль или имя пользователя. Ни в коем случае не говорите, никому свой пароль к почте, иначе злоумышленник сможет через вашу почту получить доступ ко всем сервисам и сайтам, на которых указан Ваш почтовый адрес.

Полезные советы

4) Если Вы хотите скачать какой-то материал из интернета, на сайте где не нужна регистрация, но от Вас требуют ввести адрес своей электронной почты, то, скорее всего, на Ваш адрес будут высылать рекламу или спам. В таких случаях пользуйтесь одноразовыми почтовыми ящиками.
5) Скачивайте программы либо с официальных сайтов разработчиков. Не скачивайте программы с подозрительных сайтов или с файлообменников. Так Вы уменьшите риск скачать вирус вместо программы.
6) Не нажимайте на красивые баннеры или рекламные блоки на сайтах, какими бы привлекательными и заманчивыми они не были. В лучшем случае, Вы поможете автору сайта получить деньги, а в худшем — получите вирус. Используйте плагины для браузеров, которые отключают рекламу на сайтах.
7) Если Вы работаете за компьютером, к которому имеют доступ другие люди (на роботе или в интернет кафе), не сохраняйте пароли в браузере. В противном случае, любой, кто имеет доступ к этому компьютеру, сможет зайти на сайт, используя Ваш пароль.
8) Не открывайте письма от неизвестных Вам пользователей (адресов). Или письма с оповещением о выигрыше в лотереи, в которой Вы просто не участвовали.
9) Не нажимайте на вплывающие окна, в которых написано, что Ваша учетная запись в социальной сети заблокирована. Это проделки злоумышленников! Если Вас вдруг заблокируют, Вы узнаете об этом, зайдя в эту социальную сеть, или администрация отправит Вам электронное письмо.
10) Периодическим меняйте пароли на самых важных сайтах. Так Вы уменьшите риск взлома вашего пароля.

Другие угрозы

Коммуникационные риски

Коммуникационные риски связаны с межличностными отношениями интернет-пользователей и включают в себя контакты педофилов с подростками и киберпреследования.

Контентные риски

Контентные риски связаны с потреблением информации, которая публикуется в интернете и включает в себя незаконный и непредназначенный для подростков (неподобающий) контент.

Неподобающий контент

В зависимости от культуры, законодательства, менталитета и узаконенного возраста согласия в стране определяется группа материалов, считающихся неподобающими. Неподобающий контент включает в себя материалы, содержащие: насилие, эротику и порнографию, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду анорексии и булимии, суицида, азартных игр и наркотических веществ.

Другие угрозы

Незаконный контакт - это общение между взрослым и ребенком, при котором взрослый пытается установить более близкие отношения для сексуальной эксплуатации ребенка.

Киберпреследование - это преследование человека сообщениями, содержащими оскорбления, агрессию, сексуальные домогательства с помощью интернет-коммуникаций. Также, киберпреследование может принимать такие формы, как обмен информацией, контактами или изображениями, запугивание, подражание, хулиганство (интернет-троллинг) и социальное бойкотирование.

Контакты с незнакомыми людьми

Все чаще и чаще злоумышленники используют эти каналы для того, чтобы заставить подростков (детей) выдать личную информацию

В других случаях, это могут быть педофилы, которые ищут новые жертвы

Неконтролируемые покупки

Навязчивая реклама, недобросовестные предложения, мошеннические предложения - все это ведет к тому, что пользователя очень легко обмануть и заставить купить что-то ненужное или некачественное

Кибермошенничество

Кибермошенничество — один из видов киберпреступления, целью которого является обман пользователей: незаконное получение доступа либо хищение личной информации (номера банковских счетов, паспортные данные, коды, пароли и др.), с целью причинить материальный или иной ущерб

Предупреждение кибермошенничества:

- Изучить распространенные методы мошенничества. Необходимо советоваться со взрослыми перед тем, как воспользоваться теми или иными услугами в Интернете;
- Установите на свои компьютеры антивирус или, например, персональный брандмауэр. Эти приложения наблюдают за трафиком и могут быть использованы для выполнения множества действий на зараженных системах, наиболее частым из которых является кража конфиденциальных данных.

Безопасное совершение покупок в Интернет-магазинах

1) Прежде чем совершить покупку в интернет-магазине, удостоверьтесь в его надежности;
2) Необходимо вместе познакомиться с отзывами покупателей;
3) Проверьте реквизиты и название юридического лица – владельца магазина;
4) Уточните, как долго существует магазин. Посмотреть можно в поисковике или по дате регистрации домена (сервис WhoIs)
5) Поинтересуйтесь, выдает ли магазин кассовый чек
6) Сравните цены в разных интернет-магазинах
7) Позвоните в справочную магазина
8) Обратите внимание на правила интернет-магазина
9) Выясните, сколько точно вам придется заплатит

Виды угроз психологической безопасности

Выделяют три группы угроз психологической безопасности детей и подростков в Интернете:

- нежелательные контакты (которые могут привести к сексуальному насилию)
- кибербуллинг (оскорбления, агрессивные нападки, преследования в Сети)
- «опасные» материалы (порнография, видеоролики, изображения и тексты сексуального, экстремистского характера, призывы к насилию)

Кибербуллинг — преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.

Предупреждение кибербуллинга:

1) При общении в Интернете Вы должны быть дружелюбными с другими пользователями, ни в коем случае не писать грубых слов – читать грубости также неприятно, как и слышать;
2) Необходимо правильно реагировать на обидные слова или действия других пользователей;
3) Нельзя использовать Сеть для хулиганства, распространения сплетен или угроз;

Основные виды угроз

- Интернет-зависимость
- нарушение прав человека
- проблема изоляции и утраты «Я»
- проблема в формировании идентичности

- вред физическому здоровью
- девальвация нравственности
- снижение культурного уровня
- вытеснение и ограничение традиционных форм общения
- негативные социальные влияния

Кибербуллинг и Троллинг

Кибербуллинг - это виртуальный террор, чаще всего подростковый. Получил свое название от английского слова bull - бык, с родственными значениями:

- агрессивно нападать
- задирать
- придираться
- провоцировать
- донимать
- терроризировать
- травить

На молодёжном языке, ближайший аналог - это сленговое выражение «быковать»

Кибербуллинг и Троллинг

Троллинг - размещение в Интернете (на форумах, в дискуссионных группах, блогах и др.) провокационных сообщений с целью вызвать флейм, конфликты между участниками, взаимные оскорбления и т. п.

Троллинг - нагнетание участником общения гнева, конфликта путём скрытого или явного задирания, принижения, оскорбления другого участника или участников, зачастую с нарушением правил сайта

Сексуальные домогательства

Чаще всего сексуальные домогательства в Сети исходят от ровесников детей или молодых взрослых в возрасте от 18 до 30 лет. Не всегда угроза исходит от незнакомцев, 14% преследователей - это друзья, знакомые из реальной жизни детей

Молодежь обычно игнорирует или не придает особого значения подобным сообщениям, не испытывая негативных переживаний

Виртуальные домогательства, безусловно, являются проблемой, но к встречам в офлайне такое общение приводит очень редко

Нежелательный контент

«Опасный» контент является причиной следующих проблем:

- дети невольно сталкиваются с подобными материалами во время вполне «безобидных» сессий в Интернете
- юные пользователи часто вполне компетентны для того, чтобы найти и получить доступ к запрещенному контенту

Произвольный или непроизвольный просмотр подобных материалов негативно сказывается на детской психике, поведении

Рекомендации по информационной безопасности в Интернете

1) Всегда спрашивай старших о незнакомых вещах, о которых узнаешь в Интернете. Они расскажут, что безопасно делать, а что нет.
2) Прежде чем начать дружить с кем-то в Интернете спроси у родителей, как безопасно общаться.
3) Никогда не рассказывай о себе незнакомым людям. Где ты живешь, в какой школе учишься, и номер твоего телефона должны знать только родители и друзья.
4) Никогда не отправляй свои фотографии людям, которых не знаешь лично. Компьютерный друг мог говорить о себе неправду. Ты ведь не хочешь, чтобы у незнакомого человека была твоя фотография, с которой он сможет сделать все, что захочет.
5) Не встречайся с людьми, с которыми познакомился в Интернете, без родителей. Многие люди выдают себя не за тех, кем являются на самом деле.
6) Общаясь в Интернете, будь дружелюбен с другими. Не пиши грубых слов - читать грубости так же неприятно, как и слышать. Ты можешь нечаянно обидеть человека.
7) Если тебя кто-то расстроил или обидел, обязательно расскажи об этом родителям.

Рекомендации

1) Общайтесь по веб-камере только с друзьями. Следите, чтобы ваш разговор видели только вы, потому что чужие люди могут записать видео, которое видно через веб-камеру и использовать его в своих целях.
2) Нежелательные письма от незнакомых людей называются «Спам», на них нельзя отвечать, а лучше вообще не открывать потому, что в них могут быть вирусы.
3) Если вы ответите, то люди отправившие письмо, будут знать, что ваш почтовый ящик работает и дальше посылать вам спам.
4) Не забудьте сохранить все неприятные сообщения, которые вы получили, чтобы потом показать их старшим. Они помогут вам и скажут, как правильно поступить. Не расстраивайтесь, если Вы получили плохое сообщение.
5) Если вас кто-то расстроил или обидел, расскажите все старшему.

Социальные сети и блоги

Сайты социальных сетей (например, Facebook, MySpace, Одноклассники, Вконтакте) широко используются для распространения фотографий и видео, общения с людьми и пр., так же как и блоги. В обоих случаях необходимо создавать персональный профиль для того, чтобы получить к ним доступ. Эти профили, зачастую, содержат такую конфиденциальную информацию как имя, возраст и т.д. Необязательно предоставлять эту информацию, а достаточно только указать *адрес электронной почты* и имя, которое может быть *псевдонимом*.

Нельзя распространять такую информацию, как возраст, адрес проживания, а так-же свои фотографии и видео. Многие используют **блоги** в качестве своих персональных дневников. Как правило, такие онлайн-журналы содержат значительно более широкую информацию, чем следовало бы публиковать. Крайне важно предотвратить *публикацию любых данных*, которые могли бы идентифицировать пользователя, а также содержать информацию о месте проживания, учебы и другую персональную конфиденциальную информацию. Аналогично, в некоторых социальных сетях, есть возможность обмениваться файлами с другими пользователями. Необходимо отдельно обратить внимание на то, какими файлами можно обмениваться с другими пользователями и кому он может разрешить просматривать эту информацию. Совсем не сложно, например, разместить свои фотографии, но защитить их паролем, который будет доступен только своим друзьям и семье. Родителям следует знать об этих новых сервисах, а также о том, как они работают и какие риски они представляют для пользователей.

Мобильные телефоны с выходом в Интернет

Стремительное распространение сотовых телефонов во всем мире сделало их одним из основных направлений для проведения кибер-атак за последние несколько лет. Исследование показало, что такие технологии как Bluetooth (позволяет обмениваться файлами между устройствами по беспроводному каналу) и высокоскоростной доступ в Интернет сделали сотовые телефоны очень уязвимыми для атак. В настоящее время сотовые телефоны широко используются. Соответственно, Вы сталкиваетесь с точно такими же рисками, как и при использовании ПК, подключенного к Интернету.

Сейчас широко распространены системы обмена мгновенными сообщениями для сотовых телефонов. Вы можете войти в чат в любой момент, и столкнуться с теми рисками, о которых говорили выше: кража персональных данных, педофилы, распространение вирусов и вредоносных программ и т.д.

Спам также начинает одолевать сотовые телефоны. За последние несколько лет SMS-сообщения с рекламой всех типов продуктов и сервисов наводнили сотовые телефоны во всем мире. Большая часть подобной рекламы – это реклама порнографии.

Не отвечайте на сообщения из подозрительных и неизвестных источников и не соглашались на встречу с незнакомцами.

Советы по медиабезопасности от сотовой компании «Мегафон»

При использовании коротких premium номеров SMS

- Уточняйте у Оператора (на сайте, в Абонентской службе) и на специализированных ресурсах стоимость отправки SMS
- При скачивании контента на Интернет-ресурсах внимательно читайте Условия использования сервиса, а также информацию, размещенную с символом «звездочка» (*)

При работе в сети интернет

- Устанавливайте на компьютер хорошо зарекомендовавшие себя антивирусные программы и межсетевые экраны (Firewall) и своевременно их обновляйте
- При скачивании контента внимательно читайте Условия использования сервиса, а также информацию, размещенную с символом «звездочка» (*)
- Не устанавливайте сомнительное программное обеспечение на свой компьютер / мобильный телефон.
- Не открывайте и не запускайте (*.exe) вложенные файлы неизвестного происхождения
- Будьте осторожны при всплывающих окнах, не переходите по неизвестным ссылкам
- Не отправляйте SMS для разблокировки Windows и разархивирования файлов
- При заражении компьютера вирусом-вымогателем Trojan.Winlock
- Не обращайте внимания на требование вымогателей перечислить деньги
- Зайдите на специальный ресурс Dr.Web и получите БЕСПЛАТНО коды Разблокировки
- Скачайте бесплатную утилиту Dr.Web CureIt!и избавьте свой смартфон от вредоносных объектов

- Если действия вредоносных программ сделали невозможной загрузку Вашего компьютера, скачайте бесплатно Dr.Web LiveCD! и восстановите его работоспособность
- В случае возникновения дополнительных вопросов обращайтесь на официальный форум компании «Доктор Веб» в раздел «Помощь по лечению»

Используйте наши новые услуги

- Услуга «Мобильный прайс»
- Услуга «Блокировка отправки SMS на короткие номера»
- При попытках явного и скрытого вымогательства
- Избегайте или сводите к минимуму передачу любой конфиденциальной информации (номера кредитных карточек, PIN-коды, пароли и т.д.).
- Не переводите денежные средства на номера, указанные в SMS от неизвестных или сомнительных отправителей
- При просьбах вернуть ошибочно зачисленные на Ваш лицевой счет средства предлагайте обращаться к Оператору
- Перезванивайте человеку, с которым якобы случилось несчастье, или тем, кто в настоящий момент может находиться рядом с ним, если вдруг номер вашего родственника
- При использовании голосовых premium номеров
- При неотвеченных звонках не перезванивайте на незнакомые номера (особенно международные)
- Уточняйте у Оператора (на сайте, в Абонентской службе) и на специализированных ресурсах стоимость минуты разговора
- При получении информации о выигрыше приза не звоните сразу же на указанный в сообщении короткий номер, уточните информации о проведении розыгрыша у организатора акции (на сайте, при звонке на городской номер)
- При желании помочь обратившемуся на улице человеку
- Не отдавайте телефон в руки незнакомцев, предложите самостоятельно набрать нужный номер и передать информацию.
- **При получении сообщения о задолженности по номеру, который вы не подключали**
- Обратитесь в офис обслуживания Оператора для оформления заявления о непричастности к Договору.

Безопасное использованию ресурсов сети Интернет

- Гласность, широкое обсуждение проблемы онлайн-безопасности подростков в СМИ и на государственном уровне
- Объединение усилий всех членов Интернет-сообщества, как создателей сервисов и разработчиков программных продуктов, так и простых пользователей
- Разработка и внедрение программ по формированию навыков безопасного поведения в Сети для детей и подростков
- Программы родительского контроля
- Безопасный поиск
- Программы фильтры

«Интернет-зависимости», «геймерство»

Сегодня в России все более актуальны проблемы так называемой (синонимы: интернет-аддикция, виртуальная аддикция) и зависимости от компьютерных игр («геймерство»). Первыми с ними столкнулись врачи-психотерапевты, а также компании, использующие в своей деятельности Интернет и несущие убытки, в случае, если у сотрудников появляется патологическое влечение к пребыванию онлайн.

Согласно исследованиям Кимберли Янг, предвестниками интернет-зависимости являются:

1) навязчивое стремление постоянно проверять электронную почту;
2) предвкушение следующего сеанса онлайн
3) увеличение времени, проводимого онлайн;
4) увеличение количества денег, расходуемых онлайн.

Если Вы считаете, что Ваши близкие, страдают от чрезмерной увлеченности компьютером, это наносит вред их здоровью, учебе, отношениям в обществе, приводит к сильным конфликтам в семье, то Вы можете обратиться к специалистам, занимающимся этой проблемой. Они помогут построить диалог и убедить зависимого признать существование проблемы и согласиться получить помощь. Помощь может быть оказана как в специальных терапевтических группах, так и стационарно, с использованием специальных медицинских процедур.

Безопасное использованию ресурсов сети Интернет

Эффективными способами борьбы с угрозами безопасности подростков Интернете являются внимательность и осторожность при общении в сети, а также знание и соблюдение правил безопасности в сети Интернет

Правила безопасности в сети Интернет

Такие знания подростки могу приобрести:

- на уроках информатики, обществознания и снов безопасности жизнедеятельности (ОБЖ)
- участвуя в конкурсах и других мероприятиях, посвященных безопасному пространству сети Интернет
- повышая уровень своей информационной культуры самостоятельно используя ресурсы и возможности сети Интернет и соблюдая все правила безопасного поведения

Рекомендации по безопасности

- Быть осторожными с незнакомцами. Нужно помнить что ваш собеседник может оказаться не тем, кем он себя выдает.
- Нужно помнить, что любая персональная информация может быть использована против пользователя
- Если подросток подвергся в Интернет психологическому давлению, травле, угрозам, нужно обязательно сообщить взрослым (родителям, учителям или специальные службы интернет-безопасности)

Список использованных источников

1) http://www.kaspersky.ru – антивирус «Лаборатория Касперского»;
2) http://www.onlandia.org.ua/rus/ - безопасная web-зона;
3) http://www.interneshka.net – международный онлайн-конкурс по безопасному использованию Интернета;
4) http://www.saferinternet.ru – портал Российского Оргкомитета по безопасному использованию Интернета;
5) http://content-filtering.ru – Интернет СМИ «Ваш личный Интернет»;
6) http://www.rgdb.ru – Российская государственная детская библиотека.
7) http://it-researcher.ru/pages/37/internet.pdf
8) http://tinyurl.com/nwcnqfj
9) *http://base.garant.ru/12148555/#ixzz3SCxX7hvZ*
10) *http://kakkogdagde.ru/dlya-chego-nuzhen-internet/*
11) *http://www.arinteg.ru/articles/informatsionnaya-bezopasnost-v-internete-28201.html*
12) *http://www.mediascope.ru/node/841*