Министерство образования и науки Астраханской области
Государственное автономное образовательное учреждение
Астраханской области
дополнительного профессионального образования
«Институт развития образования»

ФОРМИРОВАНИЕ ИНФОРМАЦИОННОЙ КУЛЬТУРЫ У ОБУЧАЮЩИХСЯ КАК ОСНОВА БЕЗОПАСНОГО ПОВЕДЕНИЯ В ИНТЕРНЕТ-ПРОСТРАНСТВЕ (О ПРАВИЛАХ БЕЗОПАСНОСТИ ПРИ ПОСЕЩЕНИИ ИНТЕРНЕТ) МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

Астрахань 2017

ББК 74.200.51
УДК 37.048.2

Рекомендовано научно-экспертным советом
ГАОУ АО ДПО «Институт развития образования»

Формирование информационной культуры у обучающихся как основа безопасного поведения в интернет-пространстве (О правилах безопасности при посещении сети Интернет)[Текст] : методические рекомендации./ авт.-сост. С.А. Подосинников– Астрахань: Издательство ГАОУ АО ДПО «Институт развития образования», 2017. – 50 с.

Методические рекомендации адресованы руководителям образовательных организаций, заместителям руководителей, а также педагогическим работникам, занимающимся развитием информационной культуры и пропагандой безопасного поведения в интернет-пространстве среди обучающихся.

ISBN 978-5-8087-0393-3

Содержание

ВВЕДЕНИЕ

Человечество за века своего существования создало неисчислимое количество духовных и материальных ценностей. Они представлены достижениями науки, отражены в произведениях искусства, выражены мировоззренческими теориями, иными словами, образуют кладезь духовной и материальной культуры. Передача информации об этих ценностях новому поколению и привитие ему правил обращенияс нимиявляется одной из главных задач системы школьного образования и воспитания. При этом необходимо учитывать тот факт, что, начиная со второй половины двадцатого века,процессы хранения, передачи и распространения такой информации приобрели новую специфику.Это связано с развитием общества, создавшего, в свою очередь, новые условия для развития информационных технологий и средств массовой информации. В результате чего появился новый термин *–информационное общество*, представляющее собойисторическую фазу развития цивилизации, в которой главными продуктами производства стали информация и знания. Это общество характеризуется следующими чертами:

- возрастание роли информации, знаний и информационных технологий в жизни общества;
- увеличение числа людей, занятых в сфере информационных технологий;
- создание глобального информационного пространства, обеспечивающего эффективное информационное взаимодействие людей, их доступ к мировым информационным ресурсам и удовлетворение их потребностей в информационных продуктах и услугах;
- развитие информационной экономики, появление электронного правительства, социальных сетей;виртуальное пространство становится продолжением реального.

В информационном обществе приоритет информации по сравнению с другими благами и ценностями, обретение информационными ресурсами статуса стратегических определяется также и тем, что в любой сфере деятельности, включая экономическую, политическую, социальную, преимуществами обладают те, кто обеспечен полным доступом к информации и соответствующими средствами ее получения, обработки, распространения и хранения. Информация превращается в эффективное средство управления личностью и обществом. Она также становится и оружием, что подтверждается ведущимися в последние годы информационными войнами. Полнота и надежность информации все чаще ассоциируются с властью: военной, политической, управленческой, личной.

Все перечисленное выше привело к выделению следующих факторов, влияющих на процесс современного образования.

1. Темп изменений в человеческой культуре постоянно возрастал, начиная с восемнадцатого века. В двадцатом веке онзаметно ускорился и продолжает неуклонно расти. По мере жизни одного поколения основные аспекты материальной культуры полностью меняются, включая технологии материального производства, технологии обмена и получения информации, количество научных открытий в новых сферах, а также образ жизни и жизненные ценности людей. Вхождение человечества в эпоху информационного общества обусловило смену модели «образование на всю жизнь» новым подходом – «образование в течение всей жизни». Важнейшей составляющей нового подхода стала идея непрерывного образования, охватывающего все формы, типы и уровни образования, выходящего за рамки так называемого формального образования. В новом обществе требуется новый тип образования – «опережающее». При этом учеба превращается в непрерывное пожизненное занятие. Специалистом сегодня считается уже не тот, кто один раз в жизни научился делать что-то хорошо. Специалистом становится лишь тот, кто постоянно усваивает новые знания, объем которых удваивается каждые полтора года. Таким образом, в условиях новой экономики люди должны быть готовы к кардинальным изменениям в профессиональной деятельности несколько раз в течение своей жизни. Следовательно, для всех членов общества возрастает необходимость постоянного погружения в новые информационные потоки, обновления знаний, повышения квалификации, освоения новых видов деятельности. То есть человек должен уметь учиться в течение всей своей жизни, и задача современного образования заключается уже не столько в том, чтобы дать человеку знания, сколько в том, чтобы научить его добывать информацию, извлекать из нее необходимые знания самостоятельно, используя все современные возможности.

2. Кардинальное решение этих проблем невозможно без глубокого овладения постоянно возрастающими объемами и потоками разнообразной информации. Доступ к знаниям предоставляет глобальное информационное пространство, в котором также легко можно разместить и собственную информацию. В связи с неуклонным увеличением объема информации возникает противоречие между стремительными темпами роста знаний и ограниченными возможностями их усвоения человеком. Появляется так называемый информационный потоп, являющийся следствием огромногоколичества информации,которая льется на человека из всевозможных источников: газет, телевидения, интернет-блогов, уличных баннеров. Вследствиечего в деятельности образовательныхорганизаций на первое место выходит задача обучениядетей и

подростков информационной грамотности, которая является базовым элементом информационной культуры. Она включает в себя умение формулировать информационную потребность, запрашивать, искать, отбирать, оценивать и интерпретировать информацию, в каком бы виде она ни была предоставлена. Она такжеохватываетследующие умения: представлять свою информацию, свои идеи и достигать поставленных целей; защищать собственную информацию в глобальном информационном пространстве от злонамеренных действий; защищать свое сознание как от информационных атак, предпринимаемых для индивидуальных, коммерческих целей, так и от действий, предпринимаемых властями других государств в целях развязывания глобальных информационных войн.

В свете вышесказанного актуализируется проблема обеспечения безопасности винтернет-пространстве, и прежде всего детской безопасности. Возможности, которые предоставляет информационное общество, часто используют в своих целях киберпреступники. Спамеры, хакеры, фишеры, кардеры – эти необычные названия специальностейкиберпреступников часто встречаются в СМИ и стали для нас привычными.И если хакеры старой школы ориентировали свои атаки преимущественно против корпоративных клиентов, то сегодня кибермошенники направляют свои удары и изощренные схемы обмана на рядовых граждан.

Среди тех, кто пользуется методами киберпреступников, есть не только желающие просто украсть или мошенническим способом выманить деньги у граждан, но и те, кто ведет пропаганду асоциальных, деструктивных идей и ценностей. Среди них экстремистские и террористические организации, интернет-сектанты и прочие, задачами которых является дестабилизация общества, получение неограниченной власти над частью граждан. Наиболее уязвимыми в этом отношении являются дети. В силу возрастных особенностей подрастающее поколение не всегда может адекватно оценить степень опасности. Формально ребенок находится в безопасности, но атаке со стороны злоумышленников зачастую подвергается его сознание.

Таким образом, одним из стратегическихмеханизмовобеспечения безопасности подрастающего поколения от подобных явлений является формирование у детей и подростковинформационной культуры как основы безопасного нахождения в интернет-пространстве.

ИНФОРМАЦИОННАЯ КУЛЬТУРА И СОЗДАНИЕ ИНФОРМАЦИОННОГО ОБЩЕСТВА В РОССИИ

Информатизация – организованный социально-экономический процесс создания оптимальных условий для удовлетворения информационных потребностей и реализации прав граждан и организаций на использование информационных ресурсов цивилизации с применением новых информационных технологий. Это процесс формирования информационного общества. Процесс информатизации протекает неравномерно в различных странах и характеризуется разными темпами. В последние годы во многих странах развернуты соответствующие общенациональные программы, поддерживаемые государственными субсидиями.

Составной частью и необходимым условием информатизации российского общества является информатизация образования.Информатизация образования– процесс подготовки человека к полноценной жизни в условиях современного информационного мирового сообщества, к продуктивному применению информации и знаний на основе широкого использования вычислительной техники и средств телекоммуникации.

Однако решение проблем информатизации общества невозможно без учета такого компонента, как информационная культура личности. Так, даже если будет полностью реализована потребность учреждений и организаций в компьютерной технике, обеспечена бесперебойная работа электронных коммуникаций, изданы самые совершенные законы по информации и информатизации, но при этом человек не будет подготовлен к жизни в информационном обществе, то все принятые в этой области государственные программы останутся лишь благими намерениями. Именно поэтому в подготовке человека к жизни в информационном обществе особое место должно отводиться формированию информационной культуры личности [Гендина 2002].

Наступление информационной эры, переход к качественно новым технологиям работы с информацией открывают широкие перспективы для удовлетворения информационных потребностей и запросов, вместе с тем существенно повышают требования к уровню информационной культуры личности, актуализируя тем самым задачи ее формирования.

Термин «информационная культура» в отечественных публикациях впервые появился в 70-х гг. прошлого столетия и подразумевал под собой умение ориентироваться в информационном пространстве того времени, основанном на периодических изданиях и библиотечных запасах. Но уже тогда появляется представление об информационной культуре как области культуры, связанной с функционированием информации и нацеленной на формирование информационных качеств личности; как научном

направлении и области деятельности, являющейся следствием выделения и осознания научным сообществом глобальной роли информации в становлении общества и жизнедеятельности личности.

С конца 80-х годов проблемами информационной культуры наряду с библиографоведами и библиотековедами заинтересовались обществоведы, философы, специалисты в области философии информации. С философской точки зрения информационная культура выступает как важнейший компонент духовной культуры общества в целом, различных социальных групп, отдельной личности[Гендина 2006].

В 90-х годах особое влияние на наполнение понятия «информационная культура» новым содержанием оказали работы специалистов в области информатики, вычислительной техники, новых информационных технологий. Расширяющееся использование в повседневной жизни современных технических средств, применение новейшей информационной техники и технологии определили возникновение нового типа грамотности – компьютерной. Компьютерная грамотность определяется как все то, что нужно человеку, чтобы иметь дело с компьютером, с целью функционирования в обществе, основанном на информации. Таким образом, понятие информационной культуры сужалось, что стало причиной подмены разновеликих понятий[Макаренко 2009].

В ходе развития теории информационной культуры в круг принимающих участие в ее формировании специалистов стали входить представители таких наук, как лингвистика, социология, психология, педагогика, культурология, эстетика и других. Это привело к переосмысливанию и расширению понятия «информационная культура». Однако и сегодня энтузиасты, осознавшие острую потребность информационной подготовки личности в образовательных учреждениях и пытающиеся на практике осуществить мероприятия, связанные с формированием информационной культуры тех или иных социальных групп общества, испытывают серьезные затруднения. Основная сложность связана с многозначностью самого понятия «информационная культура», вызванного полисемией лежащих в его основе базовых понятий – «информация» и «культура»[Там же].

Как и для общей культуры, для информационной культуры существует большое количество определений, которые отражают разные грани этого сложного, многомерного понятия. Приведем некоторые из них.

Наиболее общее определение рассматриваемому понятию далВ.Н.Михайловский: «Информационная культура – это новый тип общения, дающий возможность свободного выхода личности в информационное бытие; свобода выхода и доступа к информации как

на локальном, так и на глобальном уровнях; новый тип мышления, формирующийся в результате освобождения человека от рутинной информационно-интеллектуальной работы» [Михайловский 2004].

Н. И. Гендина сужает анализируемый термин:«Информационная культура – одна из составляющих общей культуры человека; совокупность информационного мировоззрения и системы знаний и умений, обеспечивающих целенаправленную самостоятельную деятельность по оптимальному удовлетворению индивидуальных информационных потребностей с использованием как традиционных, так и новых информационных технологий»[Гендина 2006].

Таким образом,данное выше понятие подразумевает готовность человека к жизни и деятельности в высокоразвитой информационной среде, умение эффективно использовать ее возможности и защищаться от ее негативных воздействий. Отсюда вытекаютосновныеумения и навыки, необходимые человеку:

- понимать закономерности информационных процессов, как в общефилософском смысле, так и в реальном, бытовом;
- уметь организовать поиск и отбор информации, необходимой для решения поставленных задач;
- уметь оценить достоверность, полноту, объективность поступающей информации;
- уметь представлять информацию в разных видах, обрабатывать ее посредством подходящих информационных (в том числе компьютерных) технологий;
- уметь применять полученную информацию для принятия решений;
- обладать навыками этического поведения при использовании информации;

Информационная культура выступает важнейшим фактором успешной профессиональной и непрофессиональной деятельности, а также социальной защищенности человека в информационном обществе. Информационная культура подразумевает осознанную свободу выбора, ограниченную культурными ценностями человеческого общества, которые передаются человеку при воспитании. Таким образом, человек с низкой культурой менее защищен в открытом информационном пространстве и легко может стать жертвой информационной атаки и влияния, направленного на получение определенных результатов[Макаренко 2009].

Как было указано в определении, культура предусматривает наличие у человека информационного мировоззрения – системы собственных взглядов на мир информации и свое место в этом мире, включая убеждения и идеалы человека и его принципы познания и информационной деятельности.

Работа с компьютером оказывает существенное влияние на формирование мышления, дисциплинирует его, способствует большей четкости, точности, строгости. Характерными чертами такого мышления является умение планировать свои действия, организовывать поиск необходимой информации, строить информационные модели объектов, процессов и явлений. Таким образом, уроки информационных технологий в школе могут заменить уроки латинского языка, активно использовавшиеся для тех же целей в системе дореволюционного образования России[Гендина 2002].

В отличие от стихийно происходящих явлений природы любая культура, в том числе и информационная, есть продукт человеческой деятельности. Человек – творец, созидатель культуры и вместе с тем ее пользователь. В этой двуединой связи с деятельностью человека заключено своеобразие информационной культуры. С одной стороны, обретение информационной культуры требует значительных усилий личности, а с другой – только информационная культура открывает современному человеку доступ к накопленным цивилизацией информационным ресурсам. Именно в связи с этим об информационной культуре человека судят не по тому, что он думает о себе сам или каким он желает казаться, а по реальным результатам его самостоятельной информационной деятельности.

Информационная культура как одно из проявлений «культуры вообще» охватывает собой сферу отношений человека, отдельных социальных групп, общества к информации. Соответственно принято различать информационную культуру личности, информационную культуру определенной социальной группы (учителей, врачей, юношества и др.), информационную культуру общества в целом[Гендина 2006].

Нарушение принципа системного подхода в определении содержания работы с информацией проявилось в монодисциплинарном характере деятельности, которая сводилась к формированию компьютерной грамотности как отдельных, обособленных друг от друга направлений. Каждый из этих компонентов информационной культуры личности обладает несомненной полезностью. Вместе с тем автономное овладение знаниями и умениями, входящими в состав каждого из этих компонентов, не способно обеспечить формирование информационной культуры личности. Такой подход неправомерен с теоретической точки зрения, так как влечет неполноту, фрагментарность, отсутствие целостного представления о феномене информационной культуры. Однако информационная культура личности не может быть сформирована и в результате лишь механического сложения знаний и умений по каждому из этих компонентов. Только органичное сочетание всех этих компонентов может обеспечить продуктивность ее формирования[Макаренко 2009].

В результате учителя формируют у учащихся непрофессиональное, «облегченное» отношение к работе с информацией.

ИНТЕРНЕТ-УГРОЗЫ И ИХ ПРОФИЛАКТИКА

Современное общество характеризуется переходом к качественно новому состоянию – информационному обществу, в котором происходит активное проникновение новых информационно-коммуникационных технологий и их возрастающее влияние на все сферы общественной жизни. Становление информационного общества с различной степенью интенсивности и результативности происходит во всем мире, в том числе и в России [Новикова 2014]. С одной стороны, новые технологии играют решающую роль в промышленном производстве, определяют экономическую и политическую динамику, с другой – компьютеры, Интернет и мобильные телефоны стали неотъемлемой частью повседневной жизни значительного числа людей [Радкевич 2009]. Как группа риска, наиболее уязвима именно молодежь, так как большую часть своего времени она пребывает во Всемирной паутине [Новикова 2014].

В настоящее время информационное пространство сети Интернет используют различные экстремистские и террористические организации, радикально настроенные группировки с целью вербовки молодежи для претворения в жизнь идеологии экстремистской направленности. Данный вид экстремизма определяется как информационный экстремизм, характеризующийся следующими общими и специфическими параметрами:

- радикальностью (экстраординарностью) действий в достижении каких-либо целей, реализации интересов;

- антисоциальностью, поскольку нарушает исторически сложившиеся (типичные), позитивные формы и модели социально-правового взаимодействия, подрывает существующий баланс интересов, создавая между ними конфликтогенное пространство взаимодействия;

- аморальностью, так как всегда идет вразрез с духовно-нравственными нормами, направлен на их нивелировку и разрушение, поскольку кризис духовно-нравственного пространства, фрагментарность его функционирования открывает простор для интенсивного развития экстремистской деятельности;

- институциональностью – он «вызревает» и институциализируется в пограничных условиях и маргинальных пространствах;

- искажением политико-правового мышления, поскольку субъект экстремистской деятельности обладает чаще всего деформированным сознанием, что обусловливает его отчуждение от социально-культурных и политико-правовых норм и ценностей;

- противоправностью результатов, поскольку функционирование информационного экстремизма в ряде случаев соответствует закону, но реализует предоставленные возможности в противоположных целях [Кубякин 2011].

Среди методов экстремистского воздействия на молодежную субпопуляцию в сети Интернет выделяют:

1. Целенаправленное дезинформирование и пропагандистское воздействие на массовое сознание населения. Цель – изменение стереотипов и сложившихся норм поведения, ценностных ориентиров, «разрыхление» или полное разрушение традиционных нравственно-культурных ценностей, осуществление культурно-идеологической экспансии через привнесение чуждых «культурных ценностей». Все это приводит к подрыву общественного самосознания и исторической памяти народа;

2. Целенаправленное дезинформирование и адресное пропагандистское воздействие на индивидуальное и групповое сознание людей. Цель – манипулирование сознанием и поведением как отдельных лиц, так и конкретных групп, как правило, играющих важную роль в формировании общественного мнения, принятии политических решений и т. д.;

3. Психофизиологическое информационное – скрытое насильственное воздействие на психику человека. Цель – изменение обыденного сознания человека, его поведения, здоровья и манипулирование им[Шувалкин 2012].

Под влиянием методов информационного экстремизма в той или иной степени оказываются все пользователи Интернета, но особенно восприимчивой к подобного рода воздействиям оказывается молодежь. О. В. Эрлих и Н. И. Цыганкова – со ссылкой на Лабораторию Касперского [http://www.kaspersky.ru/press_publications] – представили данные о том, что в России 4 миллиона детей в возрасте от 8 до 14 лет пользуются Интернетом. 78% детей указанного возрастного диапазона имеют личный профиль в социальных сетях, из них «ВКонтакте» – 86% пользователей, «Одноклассники» – 16% пользователей, «Facebook» – 4% пользователей, «Твиттер» – 2% пользователей [Эрлих 2012].

У каждого 5-го ребёнка более 100 друзей в социальных сетях.

40% детей после знакомства онлайн хотят перенести общение в реальную жизнь. 10% российских родителей знают о встречах своих детей с интернет-знакомыми.

По мнению родителей, 88% из них знают о том, чем дети занимаются в Интернете и какие сайты посещают; 92% устанавливают для детей правила нахождения в Сети.

В действительности: 40% детей не обсуждают проблему интернет-безопасности с родителями; 33% детей не рассказывают родителям о том, какие сайты посещают; 34%

родителей не устанавливают для детей никаких правил поведения в Сети; 23% родителей жалуются, что дети слишком много времени проводят в Интернете; 14% родителей не представляют, сколько времени дети тратят на Интернет[Эрлих2012].

В Сети подростков подстерегают различные опасности, к которым они зачастую неготовы: доступность нежелательного контента в социальных сетях, анонимность, возможность скрыть свой реальный образ, розыгрыши призов, платные СМС на неизвестные номера и т. д. Значительную опасность могут представлять такие явления, как заражение компьютера вредоносными программами, порнография, опасные знакомства, пропаганда насилия и экстремизма, обман и вымогательство денег.

Вредоносные программы представляют собой весьма серьезную угрозу. Как следствие заражения компьютера вредоносной программой, информация, вводимая и сохраняемая на персональном компьютере, может быть повреждена, уничтожена, переслана третьим лицам. Злоумышленникам может стать доступной различная информация, например, величина кредитного счета, пин-код и номер кредитной карты. Более того, в результате вирусного заражения полученная информация может быть использована для противоправных действий по отношению к подростку и членам его семьи, а также для оказания психологического воздействия [Эрлих2012].

Глобальная сеть часто используется различными злоумышленниками для целенаправленного введения в заблуждение граждан, то есть для дезинформации. Такая «информация» маскируется под справедливый протест против ограничения свободы выражения своего мнения и т.д. Подобные информационные «вбросы» зачастую являются экстремистской информацией. Экстремисты стараются таким образом вызвать симпатию у пользователей, расшатать их убеждения, подорвать веру в общечеловеческие ценности и в итоге привлечь на свою сторону. По мнению О.В. Эрлих и Н.И. Цыганковой,для этой цели могут быть использованы данные, позволяющие идентифицировать отношение подростка к той или иной проблеме. Данные могут быть получены из личной информации, введенной в онлайн-анкету или бланк заявки, или похищены путем взлома почтового ящика, анализа сайтов посещения и т. п.[Эрлих 2012].

Вербовщики стараются выделить наиболее восприимчивую аудиторию для привлечения новых членов своих организаций, используя различные технологии веб-сайтов (звук, видео и т. п.), онлайн-технологии (чаты, форумы). С лицами юношеского и подросткового возраста, которые кажутся наиболее заинтересованными или хорошо подходящими для выполнения асоциальной деятельности, злоумышленники входят в контакт.

Г. А. Новикова и Л. А. Новикова выделяют следующие этапы информационно-психологического воздействия экстремистской направленности:

- выявление конфликтного потенциала и существующих противоречий между различными социальными группами.

-выделение социальных групп, общественно-политических объединений, способных стать стихийным инициатором (проводником) волны протеста. На эту роль могут подходить «легко воспламеняемые» группы (в частности молодежь).

- комплексная подготовка выделенных групп к дальнейшим активным действиям, определение основных модераторов.

- адаптация реальных целей в соответствии с мерой понимания выбранных групп и их модераторов (возможна подмена понятий, навязывание ложных целей). Внушение им уверенности в практической осуществимости поставленных задач.

- обеспечение информационного превосходства навязываемых идей (вбрасывание информации в целевую среду, ее «разгон» и т.д.).

- дальнейшее расширение контингента активных участников за счет обострения конфликтной ситуации, дестабилизации обстановки [Новикова 2014].

Противодействие экстремизму осуществляется в соответствии с Федеральным законом от 25 июля 2002 г. № 114-ФЗ (в редакции от 23 ноября 2015 г.) «О противодействии экстремистской деятельности», в котором сказано, что на территории Российской Федерации запрещается распространение экстремистских материалов, их производство или хранение в целях распространения. В случаях, предусмотренных законодательством Российской Федерации, производство, хранение или распространение экстремистских материалов является правонарушением и влечет за собой ответственность. Наличие законодательных норм, к сожалению, не останавливает тех, кто пропагандирует экстремизм. Сегодня проявления такого рода во многом стали отражаться в сфере массовых коммуникаций, в частности в сети Интернет, которая хорошо освоена молодежью. С целью профилактики экстремистских проявлений актуализируется необходимость ознакомления подростков с правилами поведения в Сети.

Результаты вольного общения в Сети для подростков могут быть самыми непредсказуемыми. Для того чтобы сделать интернет-жизнь более безопасной, О. В. Эрлих и Н. И. Цыганкова предлагают познакомить учащихся с правилами поведения в Интернете, начиная с самых элементарных и на первый взгляд очевидных:

1. Настоятельно не рекомендуется разглашать пароль от своего почтового ящика или аккаунта (учетной записи), страницы в социальной сети. При невыполнении данного правила злоумышленники могут воспользоваться вашим адресом и вашей адресной

книгой для рассылки сообщений, в том числе спама, сообщений неприличного характера или экстремисткой направленности, совершения противоправных действий (мошенничества, угроз, психологического давления и др.) от вашего имени.

2. Не стоит хранить пароли на компьютере: при вирусном заражении пароли могут быть похищены.

3. Необходимо закрывать сессию (осуществлять выход) по завершении работы с аккаунтомGoogle, на странице в «ВКонтакте», «Одноклассниках» и др. При использовании чужого компьютера, в общественном месте открытая сессия делает доступной всю информацию пользователя: адресную книгу, фото- и видеодокументы, сообщения в социальной сети.

4. Не рекомендуется оставлять в публичном доступе или отправлять незнакомцам по почте, при общении в социальной сети или в чате контактную информацию: злоумышленник может выследить человека по его адресу или номеру телефона.

5. Нельзя соглашаться на уговоры незнакомых людей о личной встрече. Подобные предложения лучше игнорировать, а общение со слишком настойчивым человеком прекратить.

6. Не рекомендуется публиковать адрес своей электронной почты на каких-либо форумах, сайтах сообществ и в социальных сетях. Это может стать причиной спама.

7. Не следует переходить по ссылкам в сообщениях от неизвестных адресатов, тем более сообщать логин и пароль при переходе на другой сайт. Это небезопасно, поскольку сообщение может быть отправлено злоумышленниками.

8. Не стоит переходить по ссылкам в сообщениях с привлекательными предложениями, такими как получение эксклюзивных возможностей в социальной сети или поднятие рейтинга учетной записи. Чаще всего такие сообщения рассылают мошенники или злоумышленники для того, чтобы заставить пользователя войти на вредоносную веб-страницу или заразить его компьютер вирусом.

9. Не стоит обращать внимания на предложение бесплатных подарков, легкого заработка, сообщения о получении наследства и пр. Подобные сообщения рассылаются исключительно мошенниками. Поводом для вымогательства может стать и получение гранта на обучение в престижном заведении, и работа в модельном агентстве.

10. Не стоит соглашаться на всевозможные информационные подписки из сомнительного источника: они могут оказаться платными или содержать вредоносные программы. При этом IP-адрес вашего компьютера попадает в базу данных злоумышленников, которые могут как сами воспользоваться им, так и передать другим злоумышленникам [Эрлих2012].

Для обеспечения безопасной работы в сети Интернет стоит рекомендовать родителям использование встроенных в операционные системы и отдельно устанавливаемых антивирусных программ, в функции которых будут входить:

- фильтрация нежелательного веб-контента (ресурсов эротического, экстремистского содержания и ресурсов, пропагандирующих насилие);
- «безопасный» поиск в большинстве популярных поисковых систем;
- блокирование доступа ребенка к конкретным веб-сайтам;
- блокирование доступа ребенка к группам для взрослых в социальных сетях;
- возможность отслеживать переписку ребенка в социальных сетях и IM-чатах и ограничивать общение с подозрительными корреспондентами;
- возможность устанавливать запрет на пересылку любых персональных данных в социальных сетях и IM-чатах;
- блокирование фишинговых сайтов и порносайтов, на которые часто ведут ссылки в сообщениях спамеров;
- защита от спама.

В целом, как справедливо замечают О. В. Эрлих и Н. И. Цыганкова, общение и поведение в Интернете ничем не отличается от общения и поведения в реальной жизни. Сохранение конфиденциальной информации, критическое отношение к заманчивым предложениям от посторонних лиц, избегание случайных контактов, соблюдение правил поведения учащимися, контроль со стороны взрослых за поведением подростков и создание для них безопасной среды позволят уберечь не только учащихся от столкновения с опасными явлениями, но и общество от экстремистских проявлений, как в Интернете, так и в жизни.

ПРИНЦИПЫ ФОРМИРОВАНИЯ ИНФОРМАЦИОННОЙ КУЛЬТУРЫ

В современной психолого-педагогической наукев качестве основных общеметодологических принципов информационного образования выделяютследующие: 1) принцип культурологического подхода; 2) принцип системного подхода; 3) принцип интегративности; 4) принцип деятельностного подхода; 5) принцип технологического подхода; 6) принцип непрерывности[Гендина 2002].

*Принцип культурологического подхода*базируется на осознании глубокого взаимодействия категорий «информация» и «культура», на представлении о том, что информационная культура есть неотъемлемая часть общей культуры человека. С позиций культурологического подхода информационная культура закладывает мировоззренческие установки личности; формирует ее ценностные ориентации по отношению к информации как к элементу культуры; препятствует дегуманизации и замене духовных ценностей достижениями, вызванными к жизни научно-техническим прогрессом, беспрецедентным ростом и развитием новых информационных технологий в информационном обществе.

*Принцип системного подхода*позволяет обеспечить целостность представления феномена информационной культуры, преодолеть за счет введения единой методологической базы изолированность при рассмотрении таких его традиционных компонентов, как компьютерная грамотность, реализовать в соответствии с тезисом «целое больше, чем сумма его частей» достижение нового качества в определении содержания понятия «информационная культура» как залога эффективной деятельности по решению проблемы информационной подготовки граждан.

*Принцип интегративности*дает возможность построения единой стратегии и тактики формирования информационной культуры личности с ориентацией на органичное взаимодействие на межпредметном уровне всех образовательных дисциплин школы, каждая из которых – в соответствии со своей спецификой – призвана стать участником информационного всеобуча. Реализация данного принципа открывает перспективы гармонизации совместной работы этих социальных институтов по достижению общей цели – формированию информационной культуры личности.

*Принцип деятельностного подхода*предполагает, что формирование информационной культуры личности строится не с позиции учителя, информационного работника, пытающегося объяснить школьнику, студенту, учителю, как устроена информационная служба или компьютер, и посвятить его в тонкости информационной, компьютерной технологии, а с позиции пользователя, потребителя информации, исходя из тех информационных задач, которые он должен решать в ходе своей учебной, профессиональной или досуговой деятельности.

*Принцип технологического подхода*позволяет рассматривать формирование информационной культуры личности как педагогическую технологию, включающую определенную совокупность методов и средств, обеспечивающих достижение заданного результата. Предполагает детальное определение конечного результата и обязательный контроль его точности как основы получения продукции с заданными параметрами. Обязательными требованиями при этом являются массовость и воспроизводимость полученных результатов. Нарушение этих требований и отсутствие хотя бы одного элемента в заданной технологической цепи неизбежно влечет за собой снижение качества результатов.

Процесс формирования информационной культуры личности только тогда обретает статус технологии, когда определена программа деятельности с четко сформулированной целью, установленной последовательностью действий, ведущих к достижению поставленной цели (учебная программа); имеются средства реализации поставленной цели (учебно-методические, технические и др.); установлены требования к конечному продукту (знаниям и умениям) на каждом этапе обучения; существуют инструменты измерения уровня информационной культуры (тесты, контрольные задания и др.).

*Принцип непрерывности*предусматривает использование возможностей всех звеньев системы непрерывного образования (дошкольного, общего среднего, среднего специального, высшего, послевузовского) для формирования информационной культуры личности. При этом на каждом из этих звеньев обучение основам информационной культуры должно быть обязательным и специально организованным. Доминирующим компонентом учебных материалов должны стать сведения, формирующие технологическое знание, содержащие ответ на вопрос «Как делать?» применительно к каждому конкретному информационному продукту или процессу.

Важно использование распределенной информационно-учебной среды, включающей информационные ресурсы (фонды документов и информационных изданий, традиционные и электронные библиотечные каталоги), компьютерную технику, средства доступа к удаленным отечественным и мировым информационным ресурсам. При этом для учителя (преподавателя) принципиально важно освоение основ профессиональной работы с информацией, основных законов функционирования документальных потоков информации в обществе, приемов и методов аналитико-синтетической переработки информации, критериев эффективного поиска информации.

Важная цель воспитания – подготовка человека к продуктивному осуществлению познавательной деятельности, успешной самореализации в условиях информационного общества: формирование информационного мировоззрения личности; приобретение

знаний и умений по информационному самообеспечению их учебной, профессиональной или иной познавательной деятельности.

Кроме того,необходимо привести четыре базовых принципа общества знаний (информационного общества), провозглашенных ЮНЕСКО. Они также напрямую связаны с формированием информационной культуры личности.

1. *Всеобщий доступ к информации*

Человек, которому необходимо обеспечить доступ к информации, должен осознавать свои потребности в информации, быть способен их выражать, иметь представление о многообразных современных информационных ресурсах. Он должен уметь вести поиск необходимой информации как в традиционной (бумажной), так и в электронной среде. Эти знания и умения составляют ядро информационной грамотности и являются неотъемлемой частью информационной культуры личности.

2. *Равный доступ к качественному образованию*

Человек, освоивший информационную грамотность, способен лучше учиться, он более подготовлен к самостоятельному освоению знаний. Человек, овладевший необходимым уровнем информационной культуры, не только имеет возможность получать качественное образование, но и убежден в необходимости образования в течение всей жизни. Он владеет способами непрерывного приобретения новых знаний и умениями учиться самостоятельно. Он может работать с любой информацией, с разнородными, противоречивыми данными, обладает навыками самостоятельного (критичного), а не репродуктивного типа мышления. Все эти качества невозможны без важнейшего компонента информационной культуры личности – информационного мировоззрения.

3. *Уважение культурного многообразия*

В современном многополярном, наполненном конфликтами на расовой, национальной, языковой, религиозной почве мире человек, владеющий информационной культурой, способен к толерантному восприятию культурных явлений. Концепция формирования информационной культуры личности направлена на смягчение негативных последствий глобализации – утраты самобытных, неповторимых черт национальных культур, национальных систем образования, национальных традиций. Она соответствует лозунгу ЮНЕСКО «Все разные, все уникальные», провозглашенному во «Всемирной Декларации ЮНЕСКО по культурному разнообразию». Концепция направлена также на преодоление конфронтации двух полярных культур – технократической и гуманитарной – и позволяет обеспечить сосуществование и целостность традиционной книжной (библиотечной) и новой компьютерной (электронной) информационной культур.

4. *Свобода выражения мнений*

Свобода выражения мнений предполагает не только возможность человека заявить (письменно или устно) о своей точке зрения по какому-либо вопросу, но и несение ответственности за истинность или ложность высказанного суждения, соблюдение этических норм. Особое место в концепции формирования информационной культуры личности занимает развитие информационного мировоззрения, включающего убеждения, идеалы, принципы познания и деятельности в информационном обществе и обществе знаний. Человек, обладающий информационной культурой, может отличить информацию от дезинформации, способен критически оценивать чужое мнение и аргументированно выражать собственную точку зрения [Пидкасистый 2006].

Информационное воспитание охватывает (непосредственно и опосредованно) все стороны жизни человека и общества. В сферу и процесс информационного образования органично должны быть включены семья, школа, колледж, вуз, различные виды повышения квалификации и образования взрослых, средства массовой информации, информационные органы, учреждения культуры и искусства. Однако ведущая роль в организации информационного обучения должна быть возложена на образовательные учреждения[Там же]. Только образовательные учреждения в ряду других социальных институтов, в соответствии с существующим законодательством в образовательной сфере, способны оказывать свое каждодневное влияние на каждого учащегося, обеспечивая систематическую работу по его информационной подготовке.

МЕТОДЫ ФОРМИРОВАНИЯ ИНФОРМАЦИОННОЙ КУЛЬТУРЫ, ПРИМЕНЯЕМЫЕ В ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЯХ

Воспитание – специальная организованная деятельность педагога, направленная на развитие личности воспитанника и формирование определенных качеств – в частности на развитие информационной культуры личности. Это целенаправленный процесс воздействия на воспитуемого, заключающийся во взаимодействии, которое позволяет воспитателю осуществить такое влияние: «чем человек как человек может и должен быть» (К.Д.Ушинский). Таким образом, воспитание является одним из видов деятельности по преобразованию человека или группы людей.

Это практико-преобразующая деятельность, направленная на изменение психического состояния, мировоззрения и сознания, знания и способа деятельности, личности и ценностных ориентаций воспитуемого. При этом воспитатель должен учитывать все факторы, влияющие на воспитуемого: природные, генетические, психологические, социальные, а также его возраст и условия жизни.

Существуют различные классификации методов воспитания.

Так, например, Г. И. Щукинавыделяет три группы методов: 1) ориентированные на формирование положительного опыта поведения воспитанников в общении и деятельности; 2) направленные на достижение единства сознания и поведения воспитанников; 3) использующие поощрения и наказания [Щукина 2009]. П. И. Пидкасистый предлагает другую группировку методов воспитания: 1) формирующие мировоззрение воспитанников и осуществляющие обмен информацией; 2) организующие деятельность воспитанников и стимулирующие ее мотивы; 3) оказывающие помощь воспитанникам и осуществляющие оценку их поступков [Пидкасистый 2006]. Однако вышеозначенные классификации методов воспитания, подобно любым другим, весьма условны.

Воспитатель выбирает и использует систему методов соответственно поставленным целям. Не существует хорошего или плохого метода. Эффективность решения воспитательных задач зависит от многих факторов и условий, а также от последовательности и логики применения совокупности методов.

Для достижения целей воспитания информационной культуры необходимо:

- создание специальных условий, ситуаций и обстоятельств, которые вынуждают воспитанника изменить собственное отношение, выразить свою позицию, осуществить поступок, проявить характер;
- совместную деятельность воспитателя с воспитанником, общение, игру;

- процессы обучения и самообразования и передачи информации, социального опыта в кругу семьи, в процессе дружеского и профессионального общения.

Важной педагогической цельювоспитания является формирование информационно-методологической культуры как составляющей общей культуры человека, необходимой ему для профессиональной и общественной деятельности в информационном обществе[Гендина2006].

Достижение этой цели предусматривает решение рядаобразовательных задач, к которым относятся следующие:

- овладение учащимися представлениями об информации (информационных процессах) как одном из основополагающих понятий, составляющем фундаментсовременной картины мира;
- овладение учащимися представлениями о единстве информационных принципов строения и функционирования систем различной природы;
- овладение учащимися представлениями о роли информационных технологий в развитии общества, изменении содержания и характера деятельности человека в информационном обществе, в частности понимание принципов работы технологий, которые могут оказать негативное воздействие на образ мышления человека и побудить его к действиям, планируемым другой стороной (информационные войны);
- развитие алгоритмического мышления, создание условий для повышения креативности, формирование операционного мышления, направленного на выбор оптимальных решений;
- овладение учащимися представлениями о самообучении как об особом виде информационного процесса, привитие умений использовать информационные технологии в образовании, в изучении различных учебных предметов;
- подготовка школьников к широкому практическому использованию информационных технологий в различных сферах жизни и деятельности, овладение основными средствами компьютерных технологий;
- привитие учащимся знаний, необходимых для взаимодействия человека и общества со средствами новых информационных технологий;
- формирование понятий о культуре современного труда, стимулирование успешного обучения и личностного самоопределения[Гендина 2006].

Учащимся необходимо не столько прививать знания, сколько формировать у них умения действовать в новой информационной среде. Знания современной компьютерной среды могут устареть, но основные принципы культуры информационной деятельности

останутся. Деятельностный подход в воспитании наиболее применим к информационной культуре.

Хорошо известно, что старые подходы малоэффективны в условиях современной школы. Это подходы, связанные с формами предъявления к учащимся прямых требований, наказания, методом приучения, предполагающим демонстрацию воспитателем образца или процесса правильного выполнения действий и копирование его воспитанником[Казанцева 2008].

Федеральный государственный образовательный стандарт модифицирует модель взаимодействия между учеником и учителем. Учитель теперь не человек, который вещает «истину» ученику, а ментор, который направляет познавательную деятельность ученика в правильном направлении, помогает ему составить программу его деятельности исходя из зоны его ближайшего развития и помогает ему оценить получившийся результат. В связи с этим меняется и набор методов, применяемых в образовании и воспитании. Можно предположить, что для формирования у учеников информационной культуры наиболее применимы следующие методы:

- технология развития критического мышления через чтение и письмо (РКМЧП);
- технология педагогических мастерских;
- технология «Дебаты», дискуссионные клубы;
- технология проектной и исследовательской деятельности;
- использование современных компьютерных сервисов и сети Интернет, технологий опросов, облачных технологий;
- использование ментальных карт для объяснения и структурирования информации;
- технология кейс-стади;
- технология тренинга.

Рассмотрим эти технологии более подробно и приведем примеры, опираясь на предмет«История и обществознание».

Технология развития критического мышления через чтение и письмо(РКМЧП). Очень эффективная технология, котораяпомогает ученику анализировать и классифицировать информацию, с которой он работает. В начале урока ученики озвучивают ту информацию по теме, которой они уже владеют, и формулируют ту, которую они хотели бы узнать.Таким образом формируется цель урока – узнать определенную информацию. Далее ученик читает и анализирует самостоятельно или в группе материал,предоставленный учителем, и отмечает информацию, которую он уже

знает, новую для него информацию, интересную для него, непонятную или такую, в которой он сомневается. После обсуждения прочитанного материала ученики по заданию учителя делают свертывание информации, используя технологию кластера или ментальных карт.

Согласно отзывам учителей, эта технология хорошо работает для гуманитарных дисциплин, таких как история и обществознание, где нужно анализировать информацию и делать выводы. Поэтому РКМЧП может быть активно использована историками в целях воспитания информационной культуры.

Технология педагогических мастерских работает в ситуации, когда ученику можно поставить творческую задачу, которая опирается не столько на его знания, сколько на мироощущение и меру осознанности, то есть имеется в виду процесс самопознания. Исходя из этого, ученик должен ощутить, осознать и творчески сформировать новые для себя знания, осознать закономерности процессов или деятельности, соотнести с уже имеющимися знаниями и ощущениями. Задача педагога в данном случае состоит в том, чтобы попытаться сформировать у ребенка образ того, о чем должно быть новое знание. В истории это картина события или процесса, музыкальные фрагменты, какие-то вещи или исторические источники, которые отражают оригинальную информацию о событии, явлении, процессе. Таким образом у ученикаформируется способность самостоятельно накапливать новые знания и формулировать выводы, основываясь на начальных образах и источниках. Обязательно обращение к личному опыту учащихся, их эмоционально-чувствительной сфере. При этом включается правое полушарие – практика использования интуиции, чувства озарения.

*Технология «Дебаты». Дискуссионные клубы.*Не менее важная технология, которая помогает научиться самостоятельно мыслить, формулировать и излагать информацию, воспринимать и анализировать альтернативную информацию. Технология «Дебаты» предполагает наличие заранее определенной темы и возможность учеников самостоятельно находить и анализировать информацию по этой теме; составлять список важных аргументов, представлять информацию для презентации в аудитории. Во время дискуссии можно практиковать ситуацию разрешения спора и конфликта в аудитории, попытки свести диалектически противоречивые суждения и найти связь между ними. Все это дает хорошую возможность практиковаться в методах работы с информацией и воспитывать информационную культуру, включая культуру защиты своего мнения и дискуссии с оппонентом.

*Технология проектной и исследовательской деятельности.*Важная технология, которая способствует формированию самостоятельности ученика в информационной

деятельности: от формулирования задачи, поиска, оценки информации– до представления результатов исследования. Вся эта активность полностью возлагается на ученика с привлечением учителя только для консультирования. Посредством данной технологии прежде всего развивается умение работать с информацией.

*Использование современных компьютерных сервисов и сети Интернет. Использование технологии опроса, облачных технологий.*Имеется в виду возможность использовать для сбора информации все сервисы и ресурсы Интернета, включая каталоги электронных библиотек и хранилищ. Использование облачных технологий необходимо для хранения своей информации в Сети и доступа к ней, а также для обмена информацией с другими участниками групповой деятельности. Технология современных опросов позволяет быстро получать мнения группы по любому вопросу и анализировать данные.

Использование ментальных карт для объяснения и структурирования информации. Ментальные карты – это инструмент, позволяющий свертывать информацию, эффективно представлять ее другим, более просто освещать сложные темы. Данный инструмент хорошо подходит для проведения мозгового штурма и выявления главной информации. Работая с данной технологией, учащийся рисует связи предмета исследования с другими предметами и явлениями. Главное условие – использование ассоциаций, которые вызывает предмет. Рассматриваемый метод позволяет задействовать правое полушарие, которое ответственно за воображение, интуициюи способствует выработке альтернативных способов представления информации и обнаружения связи между предметами, явлениями. Это хорошо развивает новые аспекты информационной культуры.

Технология кейс-стади.Суть данной технологии заключается в том, что перед ученикамиставится какая-то неоднозначная ситуация, которая предполагает несколько вариантов решения. Учащимся нужно проанализировать предложенные варианты исходя из их характеристик, и принять решение по реализуемому варианту. Алгоритм работы таков:знакомство с кейсом → выявление проблемы → рассмотрение и выбор решений. Каждая группа может принять свое решение. Этот метод развивает способность к анализу, способность принимать решения исходя из имеющейся информации, умение работать в команде – совместно принимать решения, умение прослеживать причинно-следственные связи, практические навыки работы с информацией: вычленение, структурирование, выделение главного для принятия решения. Этот метод хорошо работает применительно к истории. Можно описать какое-то реальное историческое событие, проблему и предложить учащимся принять решение, выбрав его из возможных вариантов, а потом сравнить его с тем решением, которое было принятов действительности,

продемонстрировав ход мысли деятелей истории. Например, должен ли был Александр Македонский идти походом на Вавилон, отклонив предложение Дария III о мире? Мог ли он быть уверен в победе? Какие варианты у него были? Какой выбрали бы вы в этой ситуации?

Применение этих методикв комплексе позволяет педагогу решить все образовательные задачи, поставленные с целью воспитания у учеников информационной культуры, как в рамках урока, так и в процессе внеклассной работы[Казанцева 2008].

РЕКОМЕНДАЦИИ ДЛЯ РОДИТЕЛЕЙ

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ДЕТЕЙ В ИНТЕРНЕТ-ПРОСТРАНСТВЕ

Интернет постепенно проникает в наши дома, в общественные и образовательные организации, в каждое учреждение. Число пользователей Интернета в России стремительно растет и молодеет, доля молодежи и совсем юной аудитории среди пользователей Всемирной сети очень велика. Для многих из нихИнтернет становится информационной средой, без которой они не представляют себе жизни. Вместе с тем в Интернете содержатся массивы информации, которая является запрещенной для детей, так как может нанести вред их физическому и психическому здоровью, духовному и нравственному развитию[Казанцева 2008].

Согласно ст. 5 Федерального Закона от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», к информации, запрещенной для распространения среди детей, относится информация:

1) побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству;

2) способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;

3) обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным, за исключением случаев, предусмотренных настоящим Федеральным законом;

4) отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;

5) оправдывающая противоправное поведение;

6) содержащая нецензурную брань;

7) содержащая информацию порнографического характера.

Для защиты детей от опасностей в Интернете необходима активная позиция родителей. Ив этом нет ничего удивительного: ведь Интернет может быть не только прекрасным и полезным средством для обучения, отдыха или общения с друзьями. Сеть – как и реальный мир –может быть опасна: в ней существует своя преступность, хулиганство, вредительство и прочие малоприятные явления. Виртуальность общения предоставляет людям с недобрыми намерениями дополнительные возможности причинить вред детям.

В последнее время в Интернете появляется много материалов агрессивного и социально опасного содержания.Взрослым нужно помнить о существовании подобных угроз и уделять повышенное внимание вопросу обеспечения безопасности детей в Интернете. В этой связи необходимо предпринять следующие действия:

Действие 1.Установите вместе с детьми четкие правила посещения сайтов. Определите, какие сайты они могут посещать, какие – нет. Объясните вашим детям, что такое расизм, фашизм, межнациональная и религиозная вражда. Несмотря на то, что некоторые подобные материалы можно заблокировать с помощью специальных программных фильтров, не стоит надеяться на то, что вам удастся отфильтровать все подобные сайты. Выберите те, которые можно посещать вашему ребенку, и заблокируйте доступ к неподходящим материалам. Настройте параметры безопасности вашего компьютера.

Хорошей может стать идея разработать совместно с детьми Соглашение по использованию сети Интернет. В таком семейном документе вы можете описать права и обязанности каждого члена вашей семьи в сфере пользования интернет-пространством.

Действие 2.Помогите детям выбрать правильное регистрационное имя и пароль. Убедитесь в том, что они не содержат никакой личной информации.

Действие 3.Объясните детям необходимость защиты их конфиденциальности в сети Интернет. Настаивайте на том, чтобы они никогда не выдавали своего адреса, номера телефона или другой личной информации, например, места учебы или любимого места для прогулки, а также не пересылалиинтернет-знакомым свои фотографии.

Действие 4.Будьте в курсе того, с кем контактирует в Интернете ваш ребенок, старайтесь регулярно проверять список контактов своих детей, чтобы убедиться, что они лично знают всех, с кем общаются. Если ребенок интересуется контактами с людьми намного старше его, следует провести разъяснительную беседу.

Действие 5.Не позволяйте вашему ребенку встречаться с онлайн-знакомыми без вашего разрешения или в отсутствии взрослого человека. Если ребенок желает встретиться с новым интернет-другом, следует настоять на сопровождении ребенка на эту встречу. Интересуйтесь тем, куда и с кем ходит ваш ребенок.

Общение в Интернете может повлечь за собой коммуникационные риски, такие как незаконные контакты (например, груминг, кибербуллинг и др.). 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 детей 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.

Специалисты используют специальный термин «груминг», обозначающий 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.

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

Предупреждение кибербуллинга: объясните детям, что при общении в Интернете они должны быть дружелюбными с другими пользователями, ни в коем случае не писать грубых слов – читать грубости также неприятно, как и слышать. Научите детей правильно реагировать на обидные слова или действия других пользователей. Объясните детям, что нельзя использовать Сеть для хулиганства, распространения сплетен или угроз. Старайтесь следить за тем, что ваш ребенок делает в Интернете, а также наблюдайте за его настроением после пользования Сетью.

На что следует обращать внимание родителям, чтобы вовремя заметить, что ребенок стал жертвой кибербуллинга:

1) Беспокойное поведение. Даже самый замкнутый школьник будет переживать из-за происходящего и обязательно выдаст себя своим поведением. Депрессия и нежелание идти в школу – самые явные признаки того, что ребенок подвергается агрессии.

2) Неприязнь к Интернету. Если ребенок любил проводить время в Интернете и внезапно перестал это делать, следует выяснить причину. В редких случаях детям действительно надоедает проводить время в Сети. Однако в большинстве случаев внезапное нежелание пользоваться Интернетом связано с проблемами в виртуальном мире.

3) Нервозность при получении новых сообщений. Негативная реакция ребенка на звук электронного письма должна насторожить родителя. Если ребенок регулярно получает сообщения, которые расстраивают его, поговорите с ним и обсудите содержание этих сообщений.

Действие 6.Научите детей уважать других в Интернете. Убедитесь, что они знают о том, что правила хорошего поведения действуют везде – даже в виртуальном мире.

Действие 7.Настаивайте на том, чтобы дети уважали собственность других в Интернете. Объясните, что незаконное копирование и использование чужой работы – текста, музыки, компьютерных игр и других программ – является кражей.

Действие 8.Обращайте внимание, сколько времени проводят ваши дети в Интернете, чтобы вовремя заметить признаки возникающей интернет-зависимости. Предвестниками интернет-зависимости (синонимы: интернет-аддикция, виртуальная аддикция) и зависимости от компьютерных игр (геймерство) являются: навязчивое стремление постоянно проверять электронную почту; предвкушение следующего сеанса онлайн; увеличение времени, проводимого онлайн; увеличение количества денег, расходуемых онлайн. Если вы считаете, что ваши дети страдают от чрезмерной увлеченности компьютером, что наносит вред их здоровью, учебе, отношениям в обществе, приводит к сильным конфликтам в семье, то вы можете обратиться к специалистам, занимающимся этой проблемой (например, педагогам-психологам, психологам). Они помогут построить диалог и убедить зависимого признать существование проблемы и согласиться получить помощь.

Например, на сайте «Дети онлайн» (www.detionline.com) открыта линия телефонного и онлайн-консультирования для психологической и информационной поддержки детей и подростков, столкнувшихся с различными проблемами в Интернете.

Действие 9.Объясните детям, что далеко не все, что они могут прочесть или увидеть в Интернете – правда. Приучите их спрашивать о том, в чем они не уверены.

Следует объяснить детям, что нужно критически относиться к полученным из Интернета материалам, ведь опубликовать информацию в Интернете может абсолютно любой человек.

Действие 10.Контролируйте деятельность детей в Интернете с помощью современных программ. Они помогут отфильтровать вредное содержимое, выяснить, какие сайты и с какой целью посещает ребенок. Однако открытое, честное общение всегда предпочтительнее вторжения в личную жизнь.

Действие 11.Поощряйте детей делиться с вами опытом их пребывания в Интернете. Посещайте Сеть вместе с детьми. Если ваш ребенок ведет интернет-дневник, регулярно просматривайте его. Помните, что никакие технологические ухищрения не могут заменить простое родительское внимание к тому, чем занимаются дети за компьютером.

РЕКОМЕНДАЦИИ ДЛЯ РОДИТЕЛЕЙ ПО БЕЗОПАСНОМУ ИСПОЛЬЗОВАНИЮ СЕТИ ИНТЕРНЕТ СУЧЕТОМ ВОЗРАСТНЫХ И ФИЗИОЛОГИЧЕСКИХ ОСОБЕННОСТЕЙ НЕСОВЕРШЕННОЛЕТНИХ

Как показывают исследования, проводимые в сети Интернет, наиболее растущим сегментом интернет-пользователей являются дошкольники. В этом возрасте взрослые должны играть определяющую роль в обучении детей безопасному использованию Интернета.

Возраст от 5 до 6 лет

Для детей такого возраста характерен положительный взгляд на мир. Они гордятся своим умением читать и считать, а также любят делиться своими идеями. Несмотря на то, что дети в этом возрасте очень способны в использовании игр и работе с мышью, они все же сильно зависят от вас при поиске детских сайтов.

Советы по безопасности нахождения в Интернете детей данного возраста:

- Необходимо находиться рядом с детьми во время того, как они посещают интернет-пространство.
- Обязательно объясните своему ребенку, что общение в Интернете – это не реальная жизнь, а своего рода игра. При этом постарайтесь направить его усилия на познание мира.
- Добавьте детские сайты в раздел Избранное. Создайте там папку для сайтов, которые посещают ваши дети.
- Используйте средства блокирования нежелательного контента как дополнение к стандартной функции «Родительский контроль».
- Научите вашего ребенка никогда не выкладывать в Интернете информацию о себе и своей семье.
- Приучите своего ребенка сообщать вам о любых угрозах или тревогах, связанных с нахождением в сети Интернет.

Возраст от 7 до 8 лет

Как считают психологи, для детей этого возраста абсолютно естественно желание выяснить, что они могут себе позволить делать без разрешения родителей. В результате, находясь в Интернете, ребенок будет пытаться посетить те или иные сайты, а возможно и чаты, разрешение на посещение которых он не получил бы от родителей. Поэтому особенно полезны будут те отчеты, которые вам предоставит функция «Родительский контроль», или то, что вы сможете увидеть во временных файлах по использованию Интернета

(папкис:\Users\User\AppData\Local\Microsoft\Windows\TemporaryInternetFilesвоперационнойсистемеWindows).

В результате у вашего ребенка не будет ощущения, что вы глядите через его плечо на экран, однако вы будете знать, какие сайты он. Стоит понимать, что дети в данном возрасте обладают сильным чувством семьи, они доверчивы и не сомневаются в авторитетах. Дети этого возраста любят играть в сетевые игры и путешествовать по Интернету. Вполне возможно, что они используют электронную почту и могут заходить на сайты и чаты, не рекомендованные родителями.

По поводу использования электронной почты следует отметить, что в данном возрасте рекомендуется не разрешать иметь свой собственный электронный почтовый ящик, а пользоваться семейным, чтобы родители могли контролировать переписку. Помочь вам запретить ребенку использовать внешние бесплатные ящики сможет программное обеспечение со встроенной функцией«Родительский контроль».

Советы по обеспечению интернет-безопасности детей этого возраста:

- Создайте список домашних правил посещения Интернета при участии детей и требуйте его выполнения.
- Требуйте от вашего ребенка соблюдения временных норм нахождения за компьютером.
- Покажите ребенку, что вы наблюдаете за ним не потому, что вам этого хочется, а потому что вы беспокоитесь о его безопасности и всегда готовы ему помочь.
- Приучите детей к тому, что они должны посещать только те сайты, которые вы разрешили, т. е. создайте для них так называемый белый список интернет-сайтов с помощью средства «Родительский контроль». В белый список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией.
- Компьютер с выходомвИнтернет должен находиться в общей комнате под присмотром родителей.
- Используйте средства блокирования нежелательного контента как дополнение к стандартной функции «Родительский контроль».
- Создайте семейный электронный ящик, чтобы не позволить детям иметь собственные адреса.
- Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего программного обеспечения.
- Приучите детей советоваться с вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей.

- Научите детей не загружать файлы, программы или музыку без вашего согласия.
- Используйте фильтры электронной почты для блокирования сообщений от конкретных людей или сообщений, содержащих определенные слова или фразы. Подробнее о таких фильтрах вы можете узнать, например, по адресу: http://www.microsoft.com/rus/athome/security/email/fightspam.mspx.
- Не разрешайте детям использовать службы мгновенного обмена сообщениями.
- Не забывайте беседовать с детьми об их друзьях в Интернете, как если бы речь шла о друзьях в реальной жизни.
- Не накладывайте табуна вопросы половой жизни, так как в Интернете дети могут легко наткнуться на порнографию или сайты «для взрослых».
- Приучите вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам об угрозах или тревогах. Похвалите их и посоветуйте подойти снова, если возникнет подобная ситуация.

Возраст от 9 до 12 лет

В данном возрасте дети, как правило, уже наслышаны о том, какая информация существует в сети Интернет. Совершенно нормально, что они хотят это увидеть, услышать, прочесть. При этом нужно помнить, что доступ к нежелательным материалам можно легко заблокировать при помощи средств «Родительский контроль».

Советы по безопасности в этом возрасте:

- Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернету.
- Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в сети Интернет.
- Приучите детей не загружать программы без вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или нежелательное программное обеспечение.
- Создайте вашему ребенку ограниченную учетную запись для работы на компьютере.
- Настаивайте на том, чтобы дети предоставляли вам доступ к своей электронной почте, чтобы вы убедились, что они не общаются с незнакомцами.

- Объясните детям, что нельзя использовать Сеть для хулиганства, распространения сплетен или угроз.

Возраст от 13 до 17 лет

В данном возрасте родителям часто весьма сложно контролировать своих детей, так как об Интернете они знают уже значительно больше родителей. Тем не менее, именно в этом возрасте особенно важно строго соблюдать правила интернет-безопасности – соглашение между родителями и детьми. Кроме того, нужно как можно чаще просматривать отчеты о деятельности детей в Интернете. Следует обратить внимание на необходимость сохранения родительских паролей (паролей администраторов) в строгом секрете. В этом возрасте подростки активно используют поисковые машины, пользуются электронной почтой, службами мгновенного обмена сообщениями, скачивают музыку и фильмы. Мальчикам в этом возрасте больше по нраву сметать все ограничения, они жаждут грубого юмора, азартных игр, картинок «для взрослых». Девочки предпочитают общаться в чатах, при этом они гораздо более чувствительны к сексуальным домогательствам в Интернете.

Советы по обеспечению интернет-безопасности детей в указанном возрасте:

- Создайте список домашних правил посещения Интернета при участии подростков и требуйте безусловного его выполнения. Укажите список запрещенных сайтов (черный список), часы работы в Интернете. Последние могут быть легко настроены при помощи средств «Родительский контроль».
- Компьютер с подключением к Интернету должен находиться в общей комнате.
- Не забывайте беседовать с детьми об их друзьях в Интернете, о том, чем они заняты, таким образом, будто речь идет о друзьях в реальной жизни. Спрашивайте о людях, с которыми дети общаются посредством служб мгновенного обмена сообщениями, чтобы убедиться, что эти люди им знакомы.
- Используйте средства блокирования нежелательного контента как дополнение к стандартной функции «Родительский контроль».
- Будьте в курсе того, какими чатами пользуются ваши дети. Поощряйте использование моделируемых чатов и настаивайте на том, чтобы дети не общались в приватном режиме.
- Помогите подросткам защититься от спама. Научите их не выдавать в Интернете своего реального электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.

- Приучите себя знакомиться с сайтами, которые посещают подростки.
- Объясните детям, что ни в коем случае нельзя использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.
- Обсудите с подростками проблемы сетевых азартных игр и их возможные риски. Напомните, что по закону дети не могут играть в эти игры. Обеспечивать родительский контроль в Интернете можно с помощью различного программного обеспечения.

ЗАКЛЮЧЕНИЕ

Значение воспитания информационной культуры в обществе в наше время неуклонно возрастает. Это связано с непрерывным процессом преобразования нашего общества в новую историческую форму – информационное общество, для которого важность и ценность информации как таковойтрудно переоценить. Информация и знания становятся основными продуктами такого общества, над которыми работает большинство его членов. Ситуацию усугубляют другие видимые характеристики данного общества, например, информационный потоп, который представляет собой информационные массивы, обрушивающиеся на человека через все средства массовой информации. Необходимо прививать умение самостоятельно и осознанно обрабатывать эту информацию и навыки отделения «зерен от плевел» в этом информационном потоке. Нельзя забывать и об элементах информационной войны, которые все активнеепроявляются как на межгосударственном уровне в сферах идеологического влияния и управления обществом, так и на уровне бизнес-компаний, борющихся за рынки сбыта продукции.

Развитие новых технологий непрерывно увеличивает возможности доступа к информации, находящейся в глобальном информационном пространстве, и ее обработки. Неуклонно возрастает важность обеспечения защиты своей информации в глобальной пространстве, причем не только информации на материальных носителях, но и собственного разума. Мы уже научились защищать свою материальную информацию, но гораздо хуже понимаем, как нужно защищать свой разум и образ мысли от информационных вирусов, которые работают по той же схеме, что и вирусы в человеческом организме. Новые информационные технологии делают процесс проникновения таких вирусов более эффективным и массовым.

Для полного овладения информационной культурой необходимо начинать ее воспитание с детства, в школьном возрасте. Это особенно важно, потому что уровень осознанности обычного школьника не позволяет ему понять и оценить всю серьезность проблемы внешнего информационного влияния. Диалектическое мышление формируется (если формируется) на более поздних стадиях – в 20-30-летнем возрасте. Поэтому значение целенаправленного воспитания информационной культуры трудно переоценить, и роль педагога в этом процессе очень важна для того, чтобы добиться результатов, поскольку сам школьник в силу объективных причин не способен самостоятельно осознать проблему и справиться с ней.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Асеев Е. Небезопасный Интернет / Е. Асеев [Электронный ресурс] – Режим доступа: https://www.securelist.com/ru/analysis/208050652/Nebezopasnyy_internet, свободный (Дата обращения: 13.04.2017).
2. Безопасность и конфиденциальность / Образовательные программы Microsoft. [Электронный ресурс] – Режим доступа: http://windows.microsoft.com/ru-RU/windows7/help/security-privacy-user-accounts, свободный (Дата обращения: 13.04.2017).
3. БожовичЛ.И.Проблемы формирования личности: избранные психологические труды / Под ред. Д. И. Фельдштейна. – М.; Воронеж,2006.
4. ВозженниковА.В. Международный терроризм: борьба за геополитическое господство / А. В. Возженников. – М., 2005.
5. ГендинаН.И. Формирование информационной культуры личности в библиотеках и образовательных учреждениях: учебно-метод. пособие / Н.И. Гендина, Н.И.Колкова, И.Л.Скипор, Г.А.Стародубова.– М., 2002.[Электронный ресурс] – Режим доступа: http://www.ifapcom.ru/files/publications/inf_clt_lib.pdf,свободный (Дата обращения: 13.04.2017).
6. ГендинаН.И. Формирование информационной культуры личности: теоретическое обоснование и моделирование содержания учебной дисциплины / Н. И.Гендина, Н.И.Колкова, Г.А.Стародубова, Ю.В.Уленко – М., 2006. [Электронный ресурс] – Режим доступа: http://phdseminars.narod.ru/olderfiles/1/Informaccionnaya_kultura.pdf,свободный (Дата обращения: 13.04.2017).
7. ДобреньковВ.И. Социология: 3том: Социальные институты и процессы / В.И.Добреньков, А.И.Кравченко.– М., 2015.
8. Казанцева В. П. Основы информационной культуры: учебное пособие / В. П.Казанцева[и др.]. – Красноярск, 2008. [Электронный ресурс] – Режим доступа: http://files.lib.sfu-kras.ru/ebibl/umkd/208/u_course.pdf, свободный (Дата обращения: 13.04.2017).
9. КаландаровК.Х. Управление общественным сознанием. Роль коммуникативных процессов / К.Х.Каландаров.– М., 2016.
10. Компьютерная безопасность: мифы и реальность. / Образовательные программы «Лаборатории Касперского». [Электронный ресурс] – Режим доступа: www.kasperskyacademy.com/ru/view.html?id=458, свободный (Дата обращения: 13.04.2017).
11. Кривонос Г.А. Делинквентное поведение. Делинквенты. Криминальное поведение / Кривонос Г.А. (печатается по источнику). [Электронный ресурс] – Режим доступа:http://www.sevpsiport.com/psistatii/358-delinkventnoe-povedenie-kriminalnoe-povedenie-delinkventi, свободный (Дата обращения: 13.04.2017).
12. КубякинЕ.О. Особенности профилактики молодежного экстремизма в современной России /Е.О.Кубякин // Общество: политика, экономика, право. – 2011. – № 1. – С. 19-24.
13. Макаренко С. И. Информационная безопасность. Учебное пособие / С. И. Макаренко. – Ставрополь, 2009. [Электронный ресурс] – Режим доступа: http://sccs.intelgr.com/editors/Makarenko/Makarenko-ib.pdf, свободный (Дата обращения: 13.04.2017).
14. Методические рекомендации по совершенствованию пропагандистской работы в сфере противодействия распространению идеологии терроризма в субъектах Российской Федерации / под ред. В.В. Попова.– М., 2013. [Электронный ресурс] – Режим доступа: https://docviewer.yandex.ru/?url=http%3A%2F%2Fscienceport.ru%2Ffiless%2Fmetod201

3.pdf&name=metod2013.pdf&lang=ru&c=58206188433b, свободный (Дата обращения: 13.04.2017).
15. Методические материалы по профилактике терроризма и экстремизма: учебно-методическое пособие/ Составители:В.А. Сапожникова [и др.]. – Уфа, 2013.
16. Михайловский В. Н. Формирование научной картины мира и информатизация / В. Н. Михайловский. – СПб, 2014.
17. Новикова Г. А., Новикова Л.А. Профилактика экстремистских проявлений в молодежной среде:Методические рекомендации /Г.А.Новикова, Л.А.Новикова.– Архангельск, 2014. [Электронный ресурс] – Режим доступа: http://rosmetod.ru/upload/2015/01/17/08-26-23-novikova-galina_metod.-rek.-prof.-ekstrem.-proyav.-v-mol.-srede.pdf, свободный (Дата обращения: 13.04.2017).
18. Пидкасистый П. И. Педагогика: учебное пособие / П.И. Пидкасистый. – М., 2013.
19. Солдатова Г. Пойманные одной сетью: социально-психологическое исследование представлений детей и взрослых об Интернете / Г.Солдатова [и др.].– М., 2011.[Электронный ресурс] – Режим доступа: http://www.ifap.ru/library/book524.pdf, свободный (Дата обращения: 13.04.2017).
20. РадкевичА.Л. Социальные интернет-практики россиян в условиях формирования информационного общества: автореф. дис. канд. соц. наук / А.Л.Радкевич. – М., 2009.
21. Рубинштейн С.Л. Основы общей психологии / С.Л.Рубинштейн.– СПб: Питер, 2002.[Электронный ресурс] – Режим доступа: http://yanko.lib.ru/books/psycho/rubinshteyn=osnovu_obzhey_psc.pdf,свободный (Дата обращения: 13.04.2017).
22. Федеральный закон от 25.07.2002 г. в редакции от 23 ноября 2015 г. № 114-ФЗ «О противодействии экстремистской деятельности». [Электронный ресурс] – Режим доступа: http://base.garant.ru/12127578,свободный (Дата обращения: 13.04.2017).
23. ХвыляОлинтерА.И. Духовная безопасность и духовное здоровье человека, семьи, общества / А. И. Хвыля-Олинтер. – М., 2014.
24. ШтейнбухА.Г. Интернет и антитеррор:научно-популярное пособие / А.Г.Штейнбух. – М., 2013.[Электронный ресурс] – Режим доступа:https://docviewer.yandex.ru/?url=http%3A%2F%2Fvolnn.ru%2Fdata%2Ffiles%2Fantiter%2FInternet_antiterror.pdf&name=Internet_antiterror.pdf&lang=ru&c=58205f33b7ed,свободный (Дата обращения: 07.11.2016).
25. Щукина Г.И. Теория развития познавательного интереса / Г.И.Щукина. – М., 2009.
26. Эрлих О.В., ЦыганковаН.И. О современных формах работы с обучающимися образовательных учреждений по профилактике экстремистских проявлений среди несовершеннолетних:методические рекомендации /О.В.Эрлих, Н.И.Цыганкова // Письмо комитета по образованию СПБ от 15.10.2012 № 01-16-3272/12-0-1. [Электронный ресурс] – Режим доступа: https://docviewer.yandex.ru/?url=http%3A%2F%2Fkobr.spb.ru%2Fdownloads%2F727%2F1.doc&name=1.doc&lang=ru&c=58205c8d92dd, свободный (Дата обращения: 07.11.2016).

Приложение 1

ЧАСТО ЗАДАВАЕМЫЕ ВОПРОСЫ ОБИНТЕРНЕТ-БЕЗОПАСНОСТИ

Персональные компьютеры, компьютеры Mac, ноутбуки, смартфоны и планшеты все чаще подвергаются атакам вредоносных программ. Для защиты своих устройств и обеспечения безопасной работы в Интернете прежде всего необходимо хорошо знать основные категории вредоносных программ.

Что такое вредоносная программа?

Под вредоносной программой подразумевается любая программа, созданная для выполнения любого несанкционированного и, как правило, вредоносного действия на устройстве пользователя. Примеры вредоносных программ:

- вирусы;
- макровирусы для Word и Excel;
- загрузочные вирусы;
- скрипт-вирусы, включая batch-вирусы, заражающие оболочку ОС Windows, Java-приложения и т.д.;
- клавиатурные шпионы;
- программы для кражи паролей;
- троянцы-бэкдоры;
- crimeware– вредоносные программы, созданные для автоматизации совершения финансовых преступлений;
- шпионские программы;
- рекламные программы.

Чем вирус отличается от червя?

Вирус–это вредоносная программа, которая может воспроизводить сама себя и заражать файл за файлом на компьютере, а также может передаваться с одного компьютера на другой. Обычно компьютерные вирусы запрограммированы на выполнение разрушающих действий, таких как повреждение или удаление данных. Чем дольше вирус остается необнаруженным на компьютере, тем больше файлов он заразит.

Червь – это вредоносная программа, которая многократно копирует сама себя, но не наносит прямого вреда безопасности.Червь, однажды попавший на компьютер, будет искать способы перехода на другие компьютеры и носители.Если вирус является

фрагментом программного кода, который часто добавляется к обычным файлам, то червь – это самостоятельная программа.

Что такое троянская программа?

Троянская программа – это программа, которая осуществляет несанкционированные действия, направленные на уничтожение, блокирование, модификацию (или копирование) информации или нарушение работы компьютеров. В отличие от вирусов и червей троянские программы не умеют распространяться самостоятельно. Обычно пользователь не знает о вредоносных действиях троянца.

Киберпреступники используют множество троянских программ разных типов, каждый из которых предназначен для выполнения особой вредоносной функции. Наиболее распространены:

- бэкдоры;
- троянские шпионские программы;
- троянские программы для кражи паролей;
- троянские прокси-серверы, которые преобразуют ваш компьютер в средство распространения спама.

Почему троянские программы называются троянскими?

Согласно греческой мифологии, во время Троянской войны греки пошли на хитрость, чтобы проникнуть в город Трою. Они построили огромного деревянного коня и преподнесли его в подарок жителям Трои, а те, не зная, что внутри коня находятся греческие воины, внесли коня в город. Ночью греки покинули коня и открыли городские ворота, чтобы греческое войско смогло войти в Трою.

Сегодня в троянских программах применяются различные трюки для того, чтобы они могли проникнуть на устройства ничего не подозревающих пользователей.

Что такое клавиатурный шпион?

Клавиатурный шпион, или кейлоггер, – это программа, которая записывает все нажатия клавиш на клавиатуре зараженного компьютера. Киберпреступники используют клавиатурные шпионы для кражи конфиденциальных данных, например, имен пользователей, паролей, номеров и PIN-кодов кредитных карт, а также прочих сведений.

Что такое фишинг?

Фишинг– это особый вид компьютерных преступлений, который заключается в том, чтобы обманом заставить пользователя раскрыть ценную информацию, например, сведения о банковском счете или кредитных картах. Как правило, киберпреступники создают фальшивый сайт, который выглядит так же, как легальный (например, официальный сайт банка). Киберпреступники пытаются обмануть пользователя и заставить его посетить фальшивый сайт, обычно отправляя ему сообщение по электронной почте, содержащее гиперссылку на фальшивый сайт. При посещении фальшивого сайта, как правило, предлагается ввести конфиденциальные данные, например, имя пользователя, пароль или PIN-код.

Что такое шпионская программа?

Шпионские программы предназначены для сбора данных и их отправки стороннему лицу без уведомления или согласия пользователя. Как правило, шпионские программы:

- отслеживают, какие клавиши пользователь нажимает на клавиатуре;
- собирают конфиденциальную информацию, такую как пароли, номера кредитных карт, номера PIN и т.д.;
- собирают адреса электронной почты с компьютера пользователя;
- запоминают наиболее посещаемые пользователем веб-страницы.

Кроме возможного ущерба при доступе киберпреступников к этому типу информации, шпионская программа также отрицательно влияет на производительность компьютера.

Что такое drive-by-загрузка?

При drive-by-загрузке заражение компьютера происходит во время посещения веб-сайта, содержащего вредоносный код.

Киберпреступники ведут в Интернете поиск уязвимых серверов, которые можно взломать. После того как уязвимый сервер найден, киберпреступники могут разместить свой вредоносный код на веб-страницах сервера. Если операционная система компьютера или одно из приложений, работающих на компьютере, имеет незакрытую уязвимость, вредоносная программа автоматически загрузится на компьютер при посещении зараженной веб-страницы.

Что такое руткит?

Руткиты– это программы, предназначенные для сокрытия в системе определенных объектов или вредоносной активности. Очень часто руткиты используются в качестве прикрытия действий троянской программы. При установке на компьютер руткиты остаются невидимыми для пользователя и предпринимают действия, чтобы вредоносные программы не были обнаружены антивирусным программным обеспечением.

Благодаря тому, что многие пользователи входят в систему компьютера на правах администратора, а не создают отдельную учетную запись с ограниченными правами, киберпреступнику проще установить руткит.

Что такое Adware?

Рекламные программы используются либо для запуска рекламных материалов (например, всплывающих баннеров) на компьютере, либо для перенаправления результатов поиска на рекламные веб-сайты.Рекламные программы часто встраиваются в бесплатные или в условно-бесплатные программы. При загрузке бесплатной или условно-бесплатной программы в систему без уведомления или согласия пользователя может быть установлена рекламная программа.В некоторых случаях рекламная программа скрытым образом загружается с веб-сайта и устанавливается на компьютере пользователя троянцем.

Если у вас установлена не последняя версия веб-браузера, хакеры могут воспользоваться его уязвимостью, используя специальные инструменты (BrowserHijackers), которые могут загрузить рекламную программу на компьютер. BrowserHijackers могут изменять настройки браузера, перенаправлять неправильно или не полностью набранные URL-адреса на специальный сайт или менять домашнюю страницу, загружающуюся по умолчанию. Они также могут перенаправлять результаты поиска в Интернете на платные и порнографические веб-сайты.

Что такое ботнет?

Ботнет– это сеть компьютеров, контролируемых киберпреступниками с помощью троянской или другой вредоносной программы.

Что такое атака типа «отказ в обслуживании»?

Атаки типа «отказ в обслуживании» (Denial-of-Service, DoS) затрудняют или прекращают нормальное функционирование веб-сайта, сервера или другого сетевого ресурса. Хакеры добиваются этого несколькими способами, например, отправляют

серверу такое количество запросов, которое он не в состоянии обработать. Работа сервера будет замедлена, веб-страницы будут открываться намного дольше, и сервер может совсем выйти из строя, в результате чего все веб-сайты на сервере будут недоступны.

Что такое распределенная атака типа «отказ в обслуживании»?

Распределенная атака типа «отказ в обслуживании» (Distributed-Denial-of-Service, DDoS) действует аналогично обычной атаке типа «отказ в обслуживании». Однако первая осуществляется с использованием большого количества компьютеров. Обычно для распределенной атаки типа «отказ в обслуживании» хакеры используют один взломанный компьютер в качестве главного, который координирует атаку со стороны других зомби-компьютеров. Как правило, киберпреступник взламывает главный компьютер и все зомби-компьютеры, используя уязвимость в приложениях для установки троянской программы или другого компонента вредоносного кода.

Приложение 2

ПАМЯТКА ДЛЯ ДЕТЕЙ И ПОДРОСТКОВО ПРАВИЛАХ БЕЗОПАСНОГО ИСПОЛЬЗОВАНИЯ СЕТИ ИНТЕРНЕТ

1. Нормы поведения и нравственные принципы одинаковы как в виртуальном, так и в реальном мире.
2. Незаконное копирование продуктов труда других людей (музыки, игр, программ и т. д.) считается плагиатом (умышленное присвоение авторства чужого произведения).
3. Не верьте всему, что вы видите или читаете в Интернете. При наличии сомнений в правдивости какой-либо информации следует обратиться за советом к взрослым.
4. Нельзя сообщать другим пользователям Интернета личную информацию (адрес, номер телефона, номер школы, любимые места для игр и т. д.).
5. Если вы общаетесь в чатах, пользуетесь программами мгновенной передачи сообщений, играете в сетевые игры, занимаетесь в Интернете чем-то, что требует указания идентификационного имени пользователя, тогда выберите это имя вместе со взрослыми, чтобы убедиться в том, что оно не содержит никакой личной информации.
6. Интернет-друзья могут на самом деле быть не теми, за кого они себя выдают, поэтому вы не должны встречаться с интернет-друзьями без присмотра взрослых.
7. Нельзя открывать файлы, присланные неизвестными вам людьми. Эти файлы могут содержать вирусы или фото/видео с нежелательным содержанием.
8. Научитесь доверять интуиции. Если что-нибудь в Интернете вызывает у вас психологический дискомфорт, поделитесь своими сомнениями со взрослыми.

Основные правила для школьников младших классов

1. Всегда спрашивайте родителей о незнакомых вещах, встретившихся вам в Интернете. Они расскажут, что делать безопасно, а что – нет.
2. Прежде чем начать дружить с кем-то в Интернете, спросите о том, как безопасно общаться в Интернете,у родителей.
3. Никогда не рассказывайте о себе незнакомым людям: где вы живете, в какой школе учитесь, номер вашего телефона должны знать только ваши друзья и семья.
4. Не отправляйте фотографии людям, которых вы не знаете. Незнакомые люди не должны видеть ваши личные фотографии.
5. Не встречайтесь без родителей с людьми из Интернета вживую. В Интернете многие люди рассказывают о себе неправду.

6. Общаясь в Интернете, будьте дружелюбны с другими. Не пишите грубых слов, читать грубости так же неприятно, как и слышать. Вы можете нечаянно обидеть человека.
7. Если вас кто-то расстроил или обидел, обязательно расскажите родителям.

Основные правила для школьников средних классов

1. При регистрации на сайтах старайтесь не указывать личную информацию, т.к. она может стать доступной незнакомым людям. Не рекомендуется также размещать свои фотографии, тем самым давая представление о том, как вы выглядите, посторонним людям.
2. Используйте веб-камеру только при общении с друзьями. Проследите, чтобы посторонние люди не имели возможности видеть вас во время разговора, т.к. он может быть записан.
3.Нежелательные письма от незнакомых людей называются спамом. Если вы получили такое письмо, не отвечайте на него. В случае, если вы ответите на подобное письмо, отправитель будет знать, что вы пользуетесь своим электронным почтовым ящиком и будет продолжать посылать вам спам.
4. Если вам пришло сообщение с незнакомого адреса, его лучше не открывать. Подобные письма могут содержать вирусы.
5. Если вам приходят письма с неприятным и оскорбляющим вас содержанием, если кто-то ведет себя по отношению к вам неподобающим образом, сообщите об этом.
6. Если вас кто-то расстроил или обидел, расскажите об этом взрослым.

Основные правила для школьников старших классов

1. Нежелательно размещать персональную информацию в Интернете.
2. Персональная информация – это номер вашего мобильного телефона, адрес электронной почты, домашний адрес и личные фотографии.
3. Если вы публикуете фото и/или видео в Интернете – каждый может посмотреть их.
4. Не отвечайте на спам.
5. Не открывайте файлы, которые прислали неизвестные вам люди. Вы не можете знать наверняка, что содержат эти файлы – в них могут быть вирусы или фото/видео с «агрессивным» содержанием.
6. Не добавляйте незнакомых людей в свой контакт-лист в IM (Skype, Viber, WhatsApp, ICQ, MSN messenger и т.д.).
7. Помните, что виртуальные знакомые могут быть не теми, за кого себя выдают.

Приложение 3

ПАМЯТКА РОДИТЕЛЯМ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОГО НАХОЖДЕНИЯ ДЕТЕЙ В ИНТЕРНЕТЕ

В Интернете можно найти информацию и иллюстрации практически на любую тему. Необходимо обеспечить защиту детей от контактов в Интернете с нежелательными людьми, от знакомства с материалами недетской тематики или просто опасными для детской психики, от вредоносных программ и интернет-атак.

В Интернете детей подстерегает множество опасностей:

1. Контакты с нежелательными людьми, в том числе:
- угроза со стороны интернет-хулиганов;
- ловушки, расставляемые мошенниками для получения частной информации.

2. Нежелательные для просмотра или использования материалы, например:
- «взрослые» сайты;
- «пиратские» материалы.

Угрозу безопасности компьютера при пользовании Интернетом могут представлять:

- **Попутная загрузка** – когда при простом посещении веб-сайта на компьютер вашего ребенка автоматически загружается вредоносная программа.
- **Заражение через пиринговые сети (P2P)** – может предоставить доступ к компьютеру ребенка посторонним лицам.
- **Нежелательная реклама, всплывающие окна и рекламное ПО** – могут быть автоматически установлены при скачивании бесплатных программ или программ для обмена данными.

Советы родителям по интернет-безопасности: как сделать взаимодействие ребенка с Интернетом более безопасным

В интерактивном мире дети могут быть так же беззащитны, как и в реальном. Поэтому важно сделать все возможное, чтобы оградить детей от этого риска. Приведем несколько советов по интернет-безопасности, которые помогут вам защитить ваших детей.

1. Расскажите своим детям о потенциальных угрозах, с которыми они могут столкнуться в Интернете.
2. Если возможно, поставьте компьютер в общей комнате.

3. Постарайтесь проводить время за компьютером всей семьей.

4. Попросите детей рассказывать обо всем, что вызывает у них неприятные чувства или дискомфорт при посещении Интернета.

5. Ограничьте для детей доступ к компьютерным материалам.Оказать помощь в этом смогут многие антивирусные программы(например, InternetExplorer включает компонент ContentAdvisor).

6. Объясните детям, что и как им разрешено делать в Интернете, а чтозапрещено, например:

- регистрироваться в социальных сетях и на других сайтах;
- совершать покупки в Интернете;
- скачивать музыку, игры и другой контент в Интернете;
- использовать программы мгновенного обмена сообщениями;
- посещать чаты.

7. Если детям разрешено использовать программы мгновенного обмена сообщениями или посещать интернет-чаты, расскажите им об опасностях общения с людьми, которых они не знают и которым не доверяют, или отправки им сообщений.

8. Установите надежную антивирусную программу, способную защитить компьютер от вредоносных программ и хакерских атак. Многие продукты для обеспечения безопасности в Интернете сочетают в себе возможности антивирусной защиты и расширенные функции родительского контроля, которые помогают защитить детей, когда те находятся в Интернете.

Сведения об авторе-составителе:
Подосинников Сергей Александрович, ведущий научный сотрудник ГАОУ АО ДПО «Институт развития образования, кандидат психологических наук, доцент

Подосинников С.А.

ФОРМИРОВАНИЕ ИНФОРМАЦИОННОЙ КУЛЬТУРЫ У ОБУЧАЮЩИХСЯ КАК ОСНОВА БЕЗОПАСНОГО ПОВЕДЕНИЯ В ИНТЕРНЕТ-ПРОСТРАНСТВЕ
(О ПРАВИЛАХ БЕЗОПАСНОСТИ
ПРИ ПОСЕЩЕНИИ СЕТИ ИНТЕРНЕТ)
МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

Формат 60×84/16
Тираж 30 экз.

ГАОУ АО ДПО «Институт развития образования»
414000, г. Астрахань, ул.Ульяновых,4