

Педагогическим работникам

Когда речь заходит об информационной безопасности, обычно мы начинаем думать о компьютерах, сетях, интернете и хакерах. Но для образовательной среды проблема стоит шире: в ограждении воспитанника от информации, которая может негативно повлиять на его формирование и развитие, то есть о пропаганде различной направленности.

Определение термина “**информационная безопасность детей**” содержится в Законе № 436-ФЗ, регулирующем отношения, связанные с защитой детей от **информации**, причиняющей вред их здоровью и (*или*) развитию. Согласно данному закону “**информационная безопасность детей**” – это состояние защищенности, при котором отсутствует риск, связанный с причинением **информацией** вреда их здоровью и (*или*) физическому, психическому, духовному, нравственному развитию.

Обеспечение государством **информационной безопасности детей**, защита физического, умственного и нравственного развития несовершеннолетних, а также человеческого достоинства во всех аудиовизуальных медиа-услугах и электронных СМИ – требование международного права.

Закон определяет **информационную безопасность** детей как состояние защищенности, при котором отсутствует риск, связанный с причинением **информацией** (*в том числе распространяемой в сети Интернет*) вреда их здоровью, физическому, психическому, духовному и нравственному развитию.

Что такое информационная безопасность ребёнка?

Дошкольный возраст – период начальной социализации ребенка, установления взаимоотношений с различными сторонами бытия, приобщения маленького человека к миру культуры. Ребенок как никто другой нуждается в доступной, понятной и необходимой ему информации, благодаря которой он получает представление о мире, учится мыслить и анализировать, развивает свои способности, память, воображение. Основой для этого являются детские книги, телевизионные программы для детей, развивающие компьютерные игры. Но вместе с тем, всеобщая компьютеризация породила ряд проблем. Это прежде всего снижение интереса к чтению, которое является показателем общей культуры общества, и, как следствие, снижение уровня грамотности. Из-за большого потока низкопробной видеопродукции, стали утрачиваться ценности, которые накапливались веками. Причиной этой негативной тенденции является

некритичное восприятие информации, неразвитость механизмов личностной рефлексии и саморегуляции. Все эти проблемы ребенок самостоятельно решить не может. Взрослому человеку необходимо критически оценить ситуацию, научиться вычленять положительное и отсеивать отрицательное в сложившейся ситуации.

Понятие информационной безопасности

Под информационной безопасностью понимается защищенность информационной системы от случайного или преднамеренного вмешательства, наносящего ущерб владельцам или пользователям информации.

На практике важнейшими являются три аспекта информационной безопасности:

- доступность (возможность за разумное время получить требуемую информационную услугу);
- целостность (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);
- конфиденциальность (защита от несанкционированного прочтения).

Нарушения доступности, целостности и конфиденциальности информации могут быть вызваны различными опасными воздействиями на информационные компьютерные системы.

Основные угрозы информационной безопасности

Современная информационная система представляет собой сложную систему, состоящую из большого числа компонентов различной степени автономности, которые связаны между собой и обмениваются данными. Практически каждый компонент может подвергнуться внешнему воздействию или выйти из строя. Компоненты автоматизированной информационной системы можно разбить на следующие группы:

- Аппаратные средства. Это компьютеры и их составные части (процессоры, мониторы, терминалы, периферийные устройства – принтеры, контроллеры, кабели, линии связи и т.д.);
- Программное обеспечение. Это приобретенные программы, исходные, объектные, загрузочные модули; операционные системы и системные программы (компиляторы, компоновщики и др.), утилиты, диагностические программы и т.д.;

- Данные ,хранимые временно и постоянно, на дисках, флэшках, печатные, архивы, системные журналы и т.д.;
- Персонал. Пользователи, системные администраторы, программисты и др.

Опасные воздействия на компьютерную информационную систему можно подразделить на случайные и преднамеренные. Анализ опыта проектирования, изготовления и эксплуатации информационных систем показывает, что информация подвергается различным случайным воздействиям на всех этапах цикла жизни системы. Причинами случайных воздействий при эксплуатации могут быть:

- аварийные ситуации из-за стихийных бедствий и отключений электропитания;
- отказы и сбои аппаратуры;
- ошибки в программном обеспечении;
- ошибки в работе персонала;
- помехи в линиях связи из-за воздействий внешней среды.

Преднамеренные воздействия – это целенаправленные действия нарушителя. В качестве нарушителя могут выступать служащий, посетитель, конкурент, наемник. Действия нарушителя могут быть обусловлены разными мотивами:

- недовольством служащего своей карьерой;
- взяткой;
- любопытством;
- конкурентной борьбой;
- стремлением самоутвердиться любой ценой.

Можно составить гипотетическую модель потенциального нарушителя:

- квалификация нарушителя на уровне разработчика данной системы;
 - нарушителем может быть как постороннее лицо, так и законный пользователь системы;
 - нарушителю известна информация о принципах работы системы;
- нарушитель выбирает наиболее слабое звено в защите.

Наиболее распространенным и многообразным видом компьютерных нарушений является несанкционированный доступ. Несанкционированный доступ использует любую ошибку в системе защиты и возможен при нерациональном выборе средств защиты, их некорректной установке и настройке.

Проведем классификацию каналов несанкционированного доступа, по которым можно осуществить хищение, изменение или уничтожение информации:

Через человека:

- хищение носителей информации;
- чтение информации с экрана или клавиатуры;
- чтение информации из распечатки.

Через программу:

- перехват паролей;
- дешифровка зашифрованной информации;
- копирование информации с носителя.

Через аппаратуру:

- подключение специально разработанных аппаратных средств, обеспечивающих доступ к информации;
- перехват побочных электромагнитных излучений от аппаратуры, линий связи, сетей электропитания и т.д.

Особо следует остановиться на угрозах, которым могут подвергаться компьютерные сети. Основная особенность любой компьютерной сети состоит в том, что ее компоненты распределены в пространстве. Связь между узлами сети осуществляется физически с помощью сетевых линий и программно с помощью механизма сообщений. При этом управляющие сообщения и данные, пересылаемые между узлами сети, передаются в виде пакетов обмена. Компьютерные сети характерны тем, что против них предпринимают так называемые удаленные атаки. Нарушитель может находиться за тысячи километров от атакуемого объекта, при этом нападению может подвергаться не только конкретный компьютер, но и информация, передающаяся по сетевым каналам связи.

Обеспечение информационной безопасности

Формирование режима информационной безопасности – проблема комплексная.

Меры по ее решению можно подразделить на пять уровней:

1. Законодательный . Это законы, нормативные акты, стандарты и т.п. Нормативно-правовая база определяющая порядок защиты информации:

2. Морально-этический. Всевозможные нормы поведения, несоблюдение которых ведет к падению престижа конкретного человека или целой организации.

3. Административный. Действия общего характера, предпринимаемые руководством организации. Такими документами могут быть:

- приказ руководителя о назначении ответственного за обеспечение информационной безопасности;
- должностные обязанности ответственного за обеспечение информационной безопасности;
- перечень защищаемых информационных ресурсов и баз данных;
- инструкцию, определяющую порядок предоставления информации сторонним организациям по их запросам, а также по правам доступа к ней сотрудников организации.

4. Физический. Механические, электро- и электронно-механические препятствия на возможных путях проникновения потенциальных нарушителей.

5. Аппаратно-программный (электронные устройства и специальные программы защиты информации).

Принятые меры по созданию безопасной информационной системы в школе:

-Обеспечена защита компьютеров от внешних несанкционированных воздействий (компьютерные вирусы, логические бомбы, атаки хакеров и т. д.)

– Установлен строгий контроль за электронной почтой, обеспечен постоянный контроль за входящей и исходящей корреспонденцией.

– Установлены соответствующие пароли на персональные ПК.

– Используются контент-фильтры, для фильтрации сайтов по их содержанию.

Единая совокупность всех этих мер, направленных на противодействие угрозам безопасности с целью сведения к минимуму возможности ущерба, образуют систему защиты.

Специалисты, имеющие отношение к системе защиты должны полностью представлять себе принципы ее функционирования и в случае возникновения затруднительных ситуаций адекватно на них реагировать. Под защитой должна находиться вся система обработки информации.

Лица, занимающиеся обеспечением информационной безопасности, должны нести личную ответственность.

Надежная система защиты должна быть полностью протестирована и согласована. Защита становится более эффективной и гибкой, если она допускает изменение своих параметров со стороны администратора.

В заключение своего доклада хотелось бы дать некоторые рекомендации по организации работы в информационном пространстве, чтобы уберечь себя и своих близких от интернет-преступников.

Рекомендации по организации работы в информационном пространстве

1. Перед началом работы необходимо четко сформулировать цель и вопрос поиска информации.
2. Желательно выработать оптимальный алгоритм поиска информации в сети Интернет, что значительно сократит время и силы, затраченные на поиск.
3. Заранее установить временный лимит (2-3 часа) работы в информационном пространстве (просмотр телепередачи, чтение, Интернет).
4. Во время работы необходимо делать перерыв на 5-10 минут для снятия физического напряжения и зрительной нагрузки.
5. Необходимо знать 3-4 упражнения для снятия зрительного напряжения и физической усталости.
6. Работать в хорошо проветренном помещении, при оптимальном освещении и в удобной позе.
7. Не стоит легкомысленно обращаться со спам-письмами и заходить на небезопасные веб-сайты. Для интернет-преступников вы становитесь лёгкой добычей.
8. При регистрации в социальных сетях, не указывайте свои персональные данные, например: адрес или день рождения.
9. Не используйте в логине или пароле персональные данные.
10. Все это позволяет интернет-преступникам получить данные доступа к аккаунтам электронной почты, а также инфицировать домашние ПК для включения их в бот-сеть или для похищения банковских данных родителей.
11. Создайте собственный профиль на компьютере, чтобы обезопасить информацию, хранящуюся на нем.

12. Не забывайте, что факты, о которых вы узнаете в Интернете, нужно очень хорошо проверить, если выбудете использовать их в своей домашней работе. Целесообразно сравнить три источника информации, прежде чем решить, каким источникам можно доверять.

13. О достоверности информации, помещенной на сайте можно судить по самому сайту, узнав об авторах сайта.

14. Размещая информацию о себе, своих близких и знакомых на страницах социальных сетей, спросите предварительно разрешение у тех, о ком будет эта информация.

15. Не следует размещать на страницах веб-сайтов свои фотографии и фотографии своих близких и знакомых, за которые вам потом может быть стыдно.

16. Соблюдайте правила этики при общении в Интернете: грубость провоцирует других на такое же поведение.

17. Используя в своей работе материал, взятый из информационного источника (книга, периодическая печать, Интернет), следует указать этот источник информации или сделать на него ссылку, если материал был вами переработан.

Методические рекомендации и информация о мероприятиях, проектах и программах, направленных на повышение информационной грамотности педагогических работников:

<http://www.ligainternet.ru/news/> Мероприятия Лиги безопасного интернета. Лига безопасного интернета — крупнейшая и наиболее авторитетная в России организация, созданная для противодействия распространению опасного контента во всемирной сети. Лига безопасного интернета была учреждена в 2011 году при поддержке Минкомсвязи РФ, МВД РФ, Комитета Госдумы РФ по вопросам семьи женщин и детей. Попечительский совет Лиги возглавляет помощник Президента Российской Федерации Игорь Щеголев.

<http://сетевичок.рф/partneram-o-proekte> Мероприятия проекта «Сетевичок». Проект представляет собой группу онлайн-мероприятий:

- Международный квест по цифровой грамотности «Сетевичок», ориентированный на детей и подростков.
- Национальная премия за заслуги компаний и организаций в сфере информационного контента для детей, подростков и молодежи «Премия Сетевичок».

- Всероссийское исследование детей и подростков «Образ жизни российских подростков в сети».
- Конференция по формированию детского информационного пространства «Сетевичок».

http://wiki.tgl.net.ru/index.php/Педагогам_o_безопасности

- Общие рекомендации по организации мероприятий по безопасному Интернет.
- Рекомендации по проведения мероприятий со школьникам (по возрастным категориям).
- Рекомендации по организации работы с родителями.

http://wiki.edu54.ru/Педагогам_o_безопасности Портал _____ предлагает электронные ресурсы по теме “Безопасный Интернет”:

Фонд развития Интернет Информация о проектах, конкурсах, конференциях и др. по компьютерной безопасности и безопасности Интернета.

Дети России Онлайн Линия помощи. Сайт проектов Фонда Развития Интернет. Телефонное и онлайн консультирование для детей и взрослых по проблемам безопасного использования интернета и мобильной связи.

Журнал «Дети в информационном обществе» В журнале рассказывается о том, как дети и подростки используют компьютеры и интернет в школе и дома, какое влияние информационные технологии оказывают на их развитие, творческие способности, образ жизни, каков круг интересов наших детей, как они общаются и как познают окружающий мир.

Рекомендации по применению Федерального закона от 29.12.2010 г. № 436 ФЗ “О защите детей от информации, причиняющей вред их здоровью и развитию”