Активное внедрение компьютерной техники в общеобразовательные учреждения позволило создать необходимые условия для подготовки участников образовательного процесса к полноценной жизни и деятельности в информационном обществе за счет повышения качества образования посредством формирования единой информационно-образовательной среды и интенсивного внедрения информационно-коммуникационных технологий в образовательный процесс. Однако широкое применение информационных технологий в образовании испытывает ряд существенных проблем, актуальной из которых является обеспечение информационной безопасности образовательного учреждения.

Процесс обеспечения информационной безопасности можно разделить на три направления

1. Обеспечение информационной безопасности персональных компьютеров, серверов, локальной сети и информационных систем,
2. Обеспечение информационной безопасности в социальных сетях,
3. Защита учащихся от доступа к негативной информации.

**Обеспечение информационной безопасности персональных компьютеров, серверов, локальной сети и информационных систем.**

Использование компьютерных технологий в учебном процессе отвечает психофизиологическому развитию учащихся, допускает простоту в организации занятий, оказывает заметное влияние на содержание, формы и методы обучения. Например, применение мультимедийных презентаций позволяет сделать уроки более интересными, включает в процесс восприятия не только зрение, но и слух, эмоции, воображение, помогает детям глубже погрузиться в изучаемый материал, сделать процесс обучения менее утомительным, позволяет повысить эффективность и мотивацию обучения.

Использование Интернета позволяет получить доступ к ряду ценнейших первоисточников – электронные библиотеки, музеи, периодику, тематические подборки материалов, профессиональные справочники, словари, клубы по интересам. Компьютерные классы в учебных заведениях без подключения к Сети воспринимаются как неполноценные. Интернет не только дает возможность освоить простейшие и абсолютно необходимые навыки информационных коммуникаций, это также среда для общения детей и молодежи, место приложения для их творчества и самовыражения. Характерным, но далеко не единственным примером является домашняя работа, в которой ребенок создает собственную веб-страничку, где рассказывает о себе, о своей семье, о том, что его живо интересует. Внедрение Интернета в школах, безусловно, повышает уровень и качество образовательных программ: возможность получать самую последнюю информацию, внедрять дистанционные программы обучения, он-лайн тестирование, изучение иностранных языков, создавать веб-странички школ, на которых давать информацию о расписаниях, экзаменах факультативных курсах. Интернет так же создает возможность расширения кругозора школьников и их общения со своими сверстниками, в том числе за рубежом: получение разнообразной профильной информации, новостей о жизни разных стран, доступ к электронным источникам: книгам, газетам, журналам, исследованиям, публикуемым он-лайн. Однако Интернет, помимо образовательных целей, зачастую используется учащимися для развлечений: посещений чатов, игровых сайтов, сайтов сомнительного содержания: порно-сайтов, сайтов религиозных сект, террористических и криминальных организаций, сайтов с нежелательным контентом. В силу того, что помимо школы школьники проводят много времени в Интернете, он становится навязчивой идеей и негативно влияет на психику ребенка по причине сложности отслеживания посещаемых ресурсов. Другой проблемой при подключении школ к Сети является необходимый минимум сетевой защиты. Школьная сеть должна быть защищена от несанкционированного проникновения, взлома, вандализма, хищения и порчи внутренних информационных ресурсов. В силу социальной и экономической ситуации в стране двумя естественными ограничениями для построения полномасштабной системы защиты информации являются:

- относительно невысокий бюджет школьной информатизации

- отсутствие в школах квалифицированных кадров для построения системы защиты.

Поэтому крайне важно обеспечить простое, эффективное и полнофункциональное решение для построения информационной безопасности уровня школы или регионального сегмента учреждений образования.

Применение межсетевых экранов (firewall), выполняющих пакетную фильтрацию, позволяет выпускать школьников и учителей в Интернет, но не впускать в школьную сеть посторонних. Использование технологии виртуальных защищенных сетей, позволяющей скрыть информацию от посторонних, полностью исключить ее модификации, а также усилить контроль доступа, выполняемый межсетевым экраном. Часто функции пакетной фильтрации и средства виртуальных частных сетей подкрепляют средствами обнаружения проникновения, назначение которых состоит в том, чтобы поднять тревогу, если система защиты взломана или просто неправильно настроена. Полезной и обязательной мерой безопасности является антивирусная профилактика. Другой полезной, хотя менее распространенной, функцией является контентная фильтрация. Технологически контентная фильтрация реализуется различными способами, но конечная ее цель – изолировать школьника от нежелательного контента.

**Обеспечение информационной безопасности в социальных сетях**

Широкое распространение социальных сетей ставит совершенно новые задачи в сфере обеспечения безопасности образовательной среды, которые пока еще слабо осознаны. Принято считать, что социальные сети представляют собой лишь платформу распространения информации, которая генерируется самими пользователями, частными лицами. Молниеносно распространяясь, она способна создавать панические настроения, формировать точку зрения больших масс людей, часто подменяя собой классические средства массовой информации, включая те из них, которые работают в поле интернета.

В то же время зарубежные исследователи безопасности образовательной среды и работники учебных заведений выделяют важный фактор опасности социальных сетей, с которым мы почти еще не сталкиваемся. Это киберхулиганство, запугивание и психическое давление, сексуальные домогательства и другие враждебные действия, реализуемые с использованием тех самых социальных сетей. В российской, еще не сложившейся, практике такие действия часто именуются «троллингом».

В России этот феномен практически не осознан, а в Европе лишь начинают приходить к его пониманию. В то же время проблема агрессии в социальных сетях остро стоит в Азии, в первую очередь в Японии. Именно там зарегистрировано большинство случаев доведения до самоубийства путем психического давления, оказываемого в виртуальной среде. В свою очередь, накопленная в США статистика, утверждает, что в той или иной степени агрессии в виртуальном пространстве подвергались свыше 44% учащихся, а в Канаде соответствующая цифра составляет 41%.

При создании аккаунта в социальной сети любой человек неосознанно формирует свой образ, как избавленный от ряда недостатков, о которых он в себе осведомлен. Дополнительно могут добавляться вымышленные факты биографии, измененные личные данные. Таким образом, формируется проекция в виртуальной среде, которая представляет не столько личность во всей ее полноте, сколько образ того, каким себя человек хочет видеть, аватар. Полнота и зрелость этого аватара главным образом зависит от психической зрелости того, кто его создает, но еще и от его способностей описать внутренне непротиворечивую проекцию себя в виртуальном мире, что для детей и подростков, разумеется, почти невозможно – для этого требуется обладать подлинно писательским талантом. А поскольку формируемый образ дополняется вымыслом, изначально не полон – то эта проекция отличается крайней хрупкостью, еще большей, чем психика ребенка, который ее формирует. Таким образом, аватар человека в виртуальной среде общения чрезвычайно уязвим сам по себе, а при ограничении способов коммуникации только текстовыми сообщениями лишен многих естественных защитных механизмов, оставляя психику человека, который стоит за аватаром, практически обнаженной.

В зарубежной практике принято считать, что осложняющим фактором является анонимизация такой травли. Давление на психику может производиться с использованием сразу нескольких виртуальных персонажей, контролируемых одним и тем же человеком. На практике, впрочем, такое происходит совсем не так часто. Ведь описываемые конфликты являются конфликтами тех самых виртуальных проекций, в каждую из которых их создатели вкладывают разные стороны своей личности. С учетом огромной численности этих аватаров всегда найдутся те, кто канализирует в интернет свою агрессию, таким образом самоутверждаясь, в то время как другие проецируют свои слабости. Их столкновения неизбежно будут происходить с соответствующими последствиями для психики.

Очевидно, что описанная проблема не имеет технического решения. В западной практике принято призывать к созданию различных сообществ, которые могли бы солидарно противостоять виртуальной агрессии, но признается, что это лишь полумера.Законодательные методы борьбы с агрессией в социальных сетях едва ли будут перспективны, поскольку факт собственно преступления (которое еще не осознано и не описано) крайне сложно доказать. Тем не менее, эта проблематика в той или иной мере требует защиты со стороны закона хотя бы для того, чтобы повысить уровень ответственности для тех, кто безоглядно переносит все виды социальных взаимодействий в виртуальное пространство.

**Защита учащихся от доступа к негативной информации**.

В настоящее время информационные технологии используются настолько активно и прозрачно, что для современного ученика доступ к почти неограниченным объемам информации настолько же естественен, как и простое очное общение – а нередко и более привычен. Разумеется, далеко не вся информация, к которой ребенок получает доступ, безобидна: проблемы распространения порнографии, идеологических материалов, пропаганды, да и даже просто новостных потоков, которые не брезгуют размещать в средствах массовой информации негативные фотографии и видеоролики. Некоторые Интернет-ресурсы могут причинить вред здоровью и развитию детей и подростков. Одни вовлекают детей в зависимость, другие разжигают национальную рознь, третьи негативно влияют на их психическое развитие, разрушают способность к реальному общению, влияют на мировоззрение, а также предлагают различные виды мошенничества.

На государственном уровне в России принят ряд законов, который ограничивает распространение информации в интернете и СМИ. Широко известно, что ввод этих законов был воспринят неоднозначно активными пользователями интернета – прежде всего, конечно, взрослыми сознательными людьми, которые воспринимают такие законы как ограничение их свобод. И действительно, упомянутые законы слабо проработаны с точки зрения практических методов их применения, а структур, которые могли бы следить за их выполнением, по сути не создано. Поэтому едва ли стоит ожидать действенного решения проблемы контроля информации, распространяемой через интернет со стороны государства. Здесь образовательные учреждения, частные лица и, скажем, кафе, которые хотели бы предоставлять доступ в интернет своим посетителям, находятся в равной ситуации и вынуждены вырабатывать решения по ограничению доступа к информации самостоятельно.

К сожалению, арсенал средств, который мог бы быть использован для решения задач фильтрации информации, не отличается разнообразием. Наиболее эффективны технические аппаратные средства для осуществления интеллектуальной фильтрации, но их стоимость делает их совершенно недосягаемыми как для образовательных учреждений. Не следует забывать и о том, что проблема ограничения доступа к информации является комплексной. Даже если она будет успешно решена внутри отдельной школы, она все равно сохранится вне учебного заведения: дома, на улице, в пунктах общественного доступа к интернету.

Следующая стадия решения проблемы могла бы заключаться в предоставлении самими учебными заведениями информации для настройки фильтрации на уровне домашних компьютеров вплоть до организации их доступа в интернет через школьный фильтрующий сервер. Такая централизованная схема позволит определять правила доступа учеников к информации согласовано, с привлечением специалистов или волонтеров, что избавит родителей от необходимости настраивать такие же фильтры самостоятельно, для чего большинство людей обычно не обладают достаточной квалификацией. Однако, такая схема все же требует довольно высокой квалификации технических специалистов и плотной работы с родителями, хорошего уровня организации процесса.

При принятии решения о создании централизованной системы фильтрации информации логичным следующим шагом становится добавление следующего уровня: центрального хранилища правил доступа, действующего на уровне региона, который обеспечивает синхронизацию всех установленных правил фильтрации для всех действующих учебных заведений. Такие системы в России уже используются провайдерами, но они осуществляют фильтрацию лишь заведомо незаконных ресурсов по решению суда. Более широкое их распространение на административном уровне могло бы способствовать созданию единой национальной системы фильтрации доступа к нежелательным ресурсам для учебных заведений. Следует четко понимать, что любая система фильтрации информации не является абсолютно устойчивой. Специалист, или даже технически образованный пользователь, способен обойти такие преграды, если у него есть мотивация это сделать. Информация о методах обхода таких фильтров широко представлена в интернете и при необходимости легко находится. Но из этого не следует, что подобного рода механизмы фильтрации совершенно бесполезны. Они не блокируют полностью доступ к нежелательной информации, но серьезно осложняют его. Само по себе это отсекает от потребления такой информации высокий процент пользователей, не имеющих адекватной технической подготовки.

Акинина Наталья Анатольевна г. Старый Оскол МОУ СОШ №33