УДК 371.2

К ВОПРОСУ О СОДЕРЖАТЕЛЬНОМ АСПЕКТЕ ПОДГОТОВКИ БУДУЩИХ УЧИТЕЛЕЙ ИНФОРМАТИКИ В КОНТЕКСТЕ ОРГАНИЗАЦИИ БЕЗОПАСНОГО ИНФОРМАЦИОННОГО ПРОСТРАНСТВА

Никифоров О.Ю.[1], Голубев О.Б.[1]

[1]ФГБОУ ВПО «Вологодский государственный университет», Вологда, Россия, Sol_Hute_II@mail.ru; Oleg_golubev@mail.ru;

В данной статье описывается подход к построению содержания предметной подготовки будущих учителей информатики по вопросам обеспечения информационной безопасности школьников. В современной педагогике и психологии вопросы защиты ребенка от негативного информационного воздействия проработаны недостаточно глубоко. Теоретическим основам информационной безопасности школьников в глобальной сети Интернет уделяется недостаточное внимание. Также практически отсутствуют педагогические условия обеспечения информационной безопасности школьника в системе образования. В статье приведен перечень ключевых тем, важных профессиональных компетенций и дидактических условий их формирования. Отдельное внимание уделено вопросам контентной фильтрации, которая выступает в качестве центрального элемента системы защиты от нежелательного контента в образовательном учреждении. Рассмотрены модели и алгоритмы интернет-фильтрации. Включение вопросов, связанных с системами контентной фильтрации, существенно повысит результативность профессиональной подготовки будущих учителей информатики.

Ключевые слова: информационная безопасность, Интернет, Web 2.0, нежелательный контент, контентная фильтрация.

THE QUESTION OF MEANINGFUL ASPECTS OF TRAINING FUTURE TEACHERS OF COMPUTER WITHIN THE CONTEXT OF THE SECURITY OF INFORMATION SPACE

Nikiforov O.Y.[1], Golubev O.B.[1]

[1]Vologda State University, Vologda, Russia, Sol_Hute_II@mail.ru; Oleg_golubev@mail.ru;

This article describes an approach to the construction of the subject content of training future teachers of computer science for information security students. In modern pedagogy and psychology of the protection of the child from negative information influence worked deep enough. The theoretical foundations of information security students in the Internet is not paid sufficient attention. Also, there are practically no pedagogical conditions of information security student in the education system. This article provides a list of key topics that are important professional competencies and didactic conditions of their formation. Special attention is paid to the issues of content filtering, which acts as a central element of protection from inappropriate content in an educational institution. The models and algorithms of Internet filtering. The inclusion of issues related to the content filtering systems, will significantly increase the effectiveness of training future teachers of computer science.

Keywords: information security, Internet, Web 2.0, inappropriate content, content filtering.

Вместе с цифровым веком, который приходит в образование, возникают серьезные угрозы информационной безопасности школьников в сети Интернет. Эти проблемы появились одновременно с тем, как Интернет стал общедоступен. Сегодня современный школьник уже не представляет своей жизни без гаджетов и цифрового контента социальных сетей.

Неограниченный объем всевозможной информации, который сваливается на школьников в сети Интернет, не может благоприятно воздействовать на психофизиологическое состояние детей.

Проблеме зависимости от сетевых и компьютерных игр, социальных сетей, развлекательных сайтов сегодня уделяется много внимания в различных научных работах. Привязанность к Интернету и к компьютерным играм может быть настолько сильной, что у детей появляется желание жить в виртуальном мире. Ребенок часто не может контролировать себя в плане времяпрепровождения за компьютером, общение даже с самыми близкими людьми сводится к минимуму.

Симптомы интернет-зависимости:

1) уменьшение времени на прием пищи, прием пищи за компьютером;
2) потеря ощущения времени за компьютером в сети Интернет;
3) общение с незнакомыми людьми в социальных сетях более частое, чем с людьми в реальном окружающем мире;
4) игнорирование семейных и домашних обязанностей;
5) пропуск учебных занятий в школе и невыполнение домашних заданий в связи с нахождением за компьютером в Интернете;
6) невозможность сократить время пребывания в Интернете;
7) вход в Интернет с целью уйти от проблем или заглушить чувства беспомощности, вины, тревоги;
8) частые смены настроения, появление усталости, раздражительности, сильное желание вернуться за компьютер;
9) отрицание наличия зависимости от сети Интернет.

Содержательный аспект предметной подготовки учителей информатики по информационной безопасности

Сегодня у будущих педагогов, обучающихся по направлению «Педагогическое образование», необходимо формировать специальные компетенции по информационной безопасности в рамках дисциплин: «Информационные технологии», «Информационные технологии в образовании», «Педагогика», «Психология», «Теория и методика обучения». Также целесообразно рассмотреть вопрос о включении в учебные планы по различным профилям направления «Педагогическое образование» дисциплину «Информационная безопасность в образовательном учреждении». В рамках этой дисциплины познакомить студентов со следующими темами:

1) правовые основы информационной безопасности;
2) защита интеллектуальной собственности;
3) виды угроз информационного воздействия на школьников;
4) программные средства защиты информации;
5) технические средства защиты;

6) безопасность учащихся в сети Интернет.

Согласимся с Ю.И. Богатыревой, которая под компетентностью педагогов в области обеспечения информационной безопасности школьников понимает «интегративную характеристику качеств личности учителя, позволяющую ему осуществлять педагогическую деятельность в соответствии с профессиональными и социальными требованиями и обладающего мотивированной заинтересованностью к организации инфобезопасной образовательной среды на основе теоретических знаний информационной безопасности, а также практических умений, навыков и определенного опыта деятельности по недопущению вреда от опасных информационных воздействий на личность школьника в соответствии с социальными требованиями современного информационного общества» [1].

Сегодня школьный учитель должен обладать следующими личностными качествами и профессиональными компетенциями:

- знание правовых норм и законов РФ об информационной безопасности, защите персональных данных, об авторском праве;
- обучение учащихся критическому осмыслению и оцениванию информации на основе нравственных и культурных ценностей;
- умение проектировать психологически безопасную и комфортную информационную образовательную среду, проводить профилактику различных форм зависимостей от компьютера;
- опыт деятельности по подготовке сознания детей к противодействию негативным информационным воздействиям, формирование навыков критического мышления, развитие способностей к самоблокированию противоправной информации;
- навыки защиты профессионально значимой информации и противостояния угрозам информационной безопасности в профессиональной деятельности.

Для того чтобы сформировать у будущих учителей компетенцию в области обеспечения информационной безопасности, необходимо выполнять следующие дидактические условия:

- введение тематики информационной безопасности школьников в различные дисциплины профессиональной подготовки будущих педагогов;
- создание профессионально ориентированной среды обучения посредством представления содержания и технологий обучения информационной безопасности, защите персональных данных и профессиональной информации в контексте будущей педагогической деятельности;
- создание механизма для оценивания уровня сформированности рассматриваемой компетентности.

К решению вопроса организации безопасного информационного пространства в школе необходимо подойти комплексно. В школе сегодня должны работать профессионалы высоко уровня, которые способны обеспечить на техническом уровне защиту учащихся от нежелательного контента сети Интернет. Учителям и психологам необходимо проводить профилактические работы с обучающимися и их родителями, всем участникам образовательного процесса должны быть доступны информационные ресурсы по организации безопасной работы в сети Интернет. Безусловно, необходим контроль со стороны родителей за тем, сколько времени проводят их дети в Интернете и какие ресурсы они посещают.

Эффективным средством для обеспечения информационной безопасности школьников, грамотно использовать которое должны уметь будущие учителя информатики, является контентная фильтрация.

Контентную фильтрацию в образовательном учреждении можно определить как совокупность комплексных технических, программных, организационных решений для обеспечения контролируемого доступа учащихся и сотрудников школы к ресурсам всемирной паутины, а также фильтрации нежелательного контента. Выделяют два основных подхода к решению данной проблемы: локальный, который подразумевает использование специального программного фильтра на компьютере пользователя, и шлюзовый, базирующийся на централизованной аппаратно-программной фильтрации входящего трафика.

Фильтрация на уровне конкретной рабочей станции обладает большей трудоемкостью, поскольку необходимо контролировать список доступа к ресурсам на уровне каждого компьютера. В большинстве случаев такую фильтрацию может отключить пользователь самостоятельно, владеющий минимальными навыками работы с персональным компьютером.

Второй вариант предполагает организацию контроля доступа к ресурсам сети Интернет, при которой ни одна рабочая станция не может миновать программный контент-фильтр, установленный на сервере, а контроль списка доступных или запрещенных ресурсов осуществляется централизованно.

Рассмотрим структура нежелательного контента, который должен анализироваться системой контентной фильтрации любого уровня. Нежелательным контентом являются [4]: вирусы, троянские и другие вредоносные программные объекты, ссылки на фишинговые сайты, активные сетевые атаки, контент, ограниченный по причине возраста пользователя.

Фильтрация нежелательного контента осуществляется с помощью интернет-фильтра, который контролирует интернет-трафик через определение категории сайта по его

содержимому. Это особенно актуально для ресурсов, которые содержат информацию разных категорий [4]. Определение категории сайта осуществляется с использованием специальных предопределенных баз путем анализа контента страниц или через описание самого web-ресурса. Переход к технологии Web 2.0 еще больше усложнил контентную фильтрацию трафика, так как теперь данные могут передаваться отдельно от элементов оформления и нежелательная информация доходит до конечного пользователя. Необходим специальный комплексный подход к анализу такого контента.

У современного школьного учителя информатики для реализации эффективных мер по обеспечению информационной безопасности в школе должны быть сформированы соответствующие компетенции, и он обязан владеть приемами работы с программными средствами контентной фильтрации.

Отдельно необходимо рассмотреть программное обеспечение для контентной фильтрации, которое можно использовать для построения эффективной системы информационной безопасности в современной российской школе. На рынке программного обеспечения представлено большое количество решений в области контентной фильтрации.
NetPolice представляет собой настольное приложение, которое реализует защиту от нежелательного контента на рабочей станции конечного пользователя. Система использует алгоритмы динамической фильтрации, которые подразумевают анализ содержимого web-ресурса в момент обращения к нему, если контент будет определен как нежелательный, но загрузка страницы в браузере заблокируется. Для повышения эффективности работы программа использует URL-фильтрацию, при которой страница или домен могут быть маркированы как нежелательный ресурс, и последующий доступ к таким элементам блокируется [6]. Система NetPolice позволяет контролировать доступ к сервисам обмена сообщениями, к web-ресурсам с потенциально опасным и неконтролируемым содержанием, с контентом, который несовместим с задачами образовательного процесса. Данная программа является эффективным инструментом контентной фильтрации на отдельной рабочей станции и может быть рекомендована для изучения будущим учителям информатики.

Примером программного решения, предназначенного для централизованного управления сетевым трафиком, в том числе и контентной фильтрацией, является «Интернет Контроль Сервер» (ИКС) [3]. Данная система позволяет: использовать готовые шаблоны правил для школ для запрета доступа на заведомо «плохие ресурсы», анализа трафика контент-фильтром; управлять доступом пользователей; применять сертифицированный межсетевой экран, обеспечивающий безопасность от угрозы извне. Применение ИКС для организации контентной фильтрации в школе позволит развернуть эффективную защиту от

нежелательного контента на любой аппаратно-программной платформе. Владение данным программным комплексом позволит существенно повысить информационную безопасность школьников в образовательном учреждении.

Активное внедрение web-сервисов поколения 2.0. выдвигает дополнительные требования к современному школьному учителю информатики [2]. Облачные технологии могут быть использованы для конструирования нового информационного пространства школы, ключевым элементом которого является система защиты от нежелательного контента. Главным преимуществом современных web-технологий является возможность построения единого комплексного образовательного инструментария, который позволит полностью заменить все настольные прикладные программы для решения широкого круга педагогических задач на уроках информатики и ИКТ. В состав «облачного» инструментария входят: текстовые, табличные, графические web-редакторы, сервисы для генерации презентаций, виртуальных плакатов, электронных книг, лент времени, файловые хранилища, графические, видео-, аудиохостинги, агрегаторы учетных записей и прочие интернет-приложения.

В структуру «облачного» инструментария современного учителя информатики должны входить сервисы, позволяющие построить границу вокруг виртуального образовательного пространства школьника. Примером такого «облачного» решения является SkyDNS [6].

SkyDNS является «облачным» сервисом и поэтому не требует установки ни на сервер, ни на рабочую станцию конечного пользователя. Данное решение подразумевает использование адресов DNS-серверов компании, предоставляющей данный сервис, на интернет-шлюзе школы. SkyDNS позволяет блокировать доступ к опасным сайтам еще до реального обращения к их контенту. Система поддерживает актуальные «черные» и «белые» списки сайтов, которые существенно повышают эффективность контентной фильтрации. Информационную безопасность школьников можно дополнительно усилить, настроив переадресацию всех поисковых запросов на безопасный поиск самого сервиса SkyDNS.

Выводы

Сегодня остро встает вопрос о необходимости формирования компетентности педагогов в области информационной безопасности личности учащихся, как закономерный ответ на информационные угрозы. Педагог должен формировать у подрастающего поколения навыки информационной безопасности и медиаграмотности, которые позволили бы учащемуся самостоятельно оценивать опасность тех или иных ресурсов, противостоять возникающим в глобальной сети Интернет новым угрозам и рискам, самостоятельно

организовывать учебную деятельность в условиях функционирования информационной среды дистанционного обучения.

Требуется разработать единую концепцию, описывающую все аспекты безопасной работы школьника в сети Интернет. К таким аспектам можно отнести: модель угроз информационной безопасности детей в глобальной сети Интернет, психологические риски в глобальной паутине, модель организации информационной безопасности в образовательном учреждении. Но одним из ключевых элементов данной модели является организация предметной подготовки будущих педагогов (бакалавров и магистров направления «Педагогическое образование») по вопросам информационной безопасности школьников. Необходимо построить методическую систему формирования у будущих учителей специальных компетенций в области информационной безопасности. Включение вопросов, связанных с системами контентной фильтрации, существенно повысит результативность подготовки.

Список литературы

1. Богатырева Ю.И. Подходы к разработке методической системы формирования компетентности в области информационной безопасности / А.Н. Привалов // Информатика и образование. — 2012. - № 10. - С. 79-82.
2. Голубев О.Б., Никифоров О.Ю. Смешанное обучение в условиях цифровой школы // Современные проблемы науки и образования. — 2012. — № 6. — С. 374-374.
3. Интернет Контроль Сервер [Электронный ресурс]. — Режим доступа: http://xserver.a-real.ru/editions/resheniya/obrazovanie.php#tab1_content (дата обращения: 27.03.15).
4. Центр безопасного интернета в России [Электронный ресурс]. — Режим доступа: http://www.saferunet.org/expert/article/743/ (дата обращения: 27.03.15).
5. Фильтр SkyDNS для школ [Электронный ресурс]. — Режим доступа: https://www.skydns.ru/school (дата обращения: 27.03.15).
6. NetPolice Pro [Электронный ресурс]. — Режим доступа: http://netpolice.ru/filters/pro/ (дата обращения: 27.03.15).

Рецензенты:

Наимов А.Н., д.ф.-м.н., профессор, профессор кафедры информатики и математики Вологодского института права и экономики ФСИН России, г. Вологда;

Шутикова М.И., д.п.н., доцент, профессор кафедры математики и информатики ФГБОУ ВПО «Череповецкий государственный университет», г. Череповец.