Казинец Виктор Алексеевич
канд. физ.-мат. наук, доцент, заведующий кафедрой
ФГБОУ ВО «Тихоокеанский государственный университет»
г. Хабаровск, Хабаровский край

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ПЕДАГОГИЧЕСКОЕ ОБРАЗОВАНИЕ

Аннотация: *в статье рассмотрены вопросы подготовки педагогов, студентов педагогического института и педагогического колледжа Хабаровского края в области информационной безопасности.*

Ключевые слова*: информация, цифровизация, информационные технологии, киберугроза, киберпреступление.*

В рамках программы цифровизации системы образования и активного внедрения информационных технологий в процесс обучения все более важными становятся вопросы информационной безопасности пользователей Интернета и социальных сетей. Данные вопросы рассматриваются на разных уровнях, в частности на парламентских слушаниях в Совете Федерации 24 мая 2017 года на заседании Комитета Совета Федерации по конституционному законодательству и государственному строительству рассматривался вопрос «Актуальные вопросы обеспечения безопасности и развития детей в информационном пространстве». Участники парламентских слушаний на данную тему, рассмотрев вопросы обеспечения безопасности и развития детей в информационном пространстве, констатируют, что информационно-телекоммуникационная сеть Интернет стала неотъемлемой частью нашей жизни и одним из ключевых источников информации. В настоящее время многочисленную и крайне активную часть его аудитории составляют дети. В частности, очень высок процент школьников среди пользователей социальных сетей.

Участники парламентских слушаний полагают, что в данной сфере имеются следующие проблемы:

1) низкая грамотность детей в вопросах безопасного поведения в интернет-пространстве;

2) опережающее использование детьми интернет-сервисов по сравнению с началом их систематизированного обучения компьютерной грамотности;

3) ненадлежащая организация защиты детей от противоправного контента в образовательных организациях, нехватка в них компетентных специалистов в области информационной безопасности;

4) недостаточность реализуемых дополнительных профессиональных программ для педагогических работников, занятых в сфере информационных технологий;

5) отсутствие должного контроля за соблюдением законодательства владельцами сайтов, провайдерами хостинга и операторами связи, оказывающими услуги по предоставлению доступа к сети Интернет;

6) ненадлежащее применение административных и организационных мер, технических и программно-аппаратных средств защиты детей от вредной информации в местах, доступных для детей;

7) необходимость повышения степени вовлеченности родителей в обеспечение детской безопасности в сети Интернет; недостаточность системной информационно-просветительской работы, направленной на профилактику интернет-зависимости, информирование детей и родителей о безопасном поведении при использовании информационно-коммуникационных технологий;

8) отсутствие системы мер по противодействию распространению материалов экстремистской направленности, пропаганде молодежных суицидов в социальных сетях;

9) нехватка развивающего и обучающего контента в сети Интернет, интересного детям, а также его пропаганды.

Отмечая важность вышеуказанных проблем, связанных с обеспечением информационной безопасности и развития детей в информационном пространстве, участники парламентских слушаний подчёркивают, что в сфере регулирования деятельности в Интернете в целом имеется качественная правовая база. Тем не

менее следует признать, что многие нынешние проблемы возникают из-за недостаточной эффективности использования уже существующих правовых инструментов. При этом участники слушаний определили направления деятельности педагогической общественности в области обеспечения информационной безопасности детей при их работе с информационными ресурсами. Мы с 2015 года внимательно следим, как меняется уровень образования в области информационной безопасности педагогической общественности Хабаровского края. С этой целью ежегодно проводится анкетирование и обсуждение по вопросам обеспечения информационной безопасности детей. Обычно анкетируется группа порядка 50 человек, выборка недостаточно репрезентативна, но позволяет оценить уровень компетентности анкетируемых и динамику изменения отношения к вопросам информационной безопасности.

Мы попробовали определить, насколько педагогическое сообщество – учителя, студенты педагогических вузов, студенты средних учебных заведений – разбирается и сможет помочь ориентироваться школьникам в сложившейся информационной среде и какие основные социальные сети ему интересны.

Первая группа вопросов была связана с существующей нормативно-правовой системой, регламентирующей жизнь и работу в информационном пространстве. Мы попытались определить, какие федеральные законы знакомы нашей аудитории, с какими федеральными законами они сталкивались в своей деятельности и в быту. Нас интересовали следующие законы:

1. «Об информации, информационных технологиях и о защите информации».

2. «О персональных данных».

3. «О защите детей от информации, причиняющей вред их здоровью и развитию».

4. «О государственной тайне».

5. «О коммерческой тайне».

6. «Об электронной числовой подписи».

7. «Об авторском праве и смежных правах».

По просьбе учителей был добавлен пункт о знакомстве с Гражданским кодексом Российской Федерации, так как кодекс позволяет определиться с авторскими правами на учебно-методические материалы, разработанные на рабочем месте. Из 50 опрошенных учителей только 3 учителя слышали о первом законе (в опросе участвовали учителя гуманитарного профиля), с 4-м, 5-м, 6-м законами не знакомы все 50 опрошенных.

С законами 2 и 3 знакомы в той или иной степени все учителя, в последующих обсуждениях мы выяснили, что с этими законами учителя сталкиваются в своей повседневной деятельности, хотя о многом, связанном с этими законами, рассуждают на уровне «здравого смысла». Выяснилось, что фактически все учителя не умеют защищать свои имущественные и авторские права, хотя фактически все создают методические пособия, разрабатывают дидактические материалы, а некоторые создают дистанционные курсы по своим дисциплинам. Следует отметить, что аналогичные опросы мы проводили и в 2015 году, и результаты были несколько хуже, то есть учителям приходится не только работать в информационной среде, но и изучать законы, регламентирующие жизнь в этой среде. Опрос показал, что подготовка учителей педагогического профиля в области информационной безопасности явно недостаточна. Необходимо как в рамках базового образования, так и на курсах подготовки и переподготовки учителей обратить внимание на их ознакомление с законодательной базой, касающейся информационной безопасности. Кстати, в сети появились достаточно хорошие курсы, позволяющие организовать подготовку учителей в этой области. К сожалению, прохождение этих курсов не отражается на зарплате учителя. В 2018 году мы повторно провели тестирование студентов педагогического института и задали им те же вопросы, что и учителям о существующей нормативно-правовой системе.

Выяснилось, что результаты фактически не отличаются от результатов учителей, хотя при обсуждении выяснилось, что студенты осведомлены гораздо лучше учителей о применении этих законов на практике. Студенты средних учебных заведений могут привести множество примеров применения законов,

взятых из Интернета (при этом непроверенных), но затрудняются говорить даже о правилах своего поведения в социальных сетях.

Вторая группа вопросов была связана с киберугрозами.

Киберугроза – это незаконное проникновение или угроза вредоносного проникновения в виртуальное пространство для достижения политических, социальных или иных целей. Киберугроза может воздействовать на информационное пространство компьютера, в котором находятся сведения, хранятся материалы физического или виртуального устройства. Атака обычно поражает носитель данных, специально предназначенный для их хранения, обработки и передачи личной информации пользователя.

К киберугрозам анкетируемые отнесли:

1. Хищения через Интернет и мобильный банкинг.
2. Программы-вымогатели.
3. Использование Интернета в террористических целях.
4. Хищение персональных данных.
5. Манипулирование в социальных сетях.
6. Баннеры и угрозы, связанные с ними.
7. Интернет-зависимость.
8. Компьютерные игры.
9. Киберунижение.
10. Экстремизм.
11. Вирусы.

Все группы анкетируемых подробно и с примерами говорили о киберугрозах и киберпреступлениях.

При рассмотрении частных примеров выяснилось, что никто не знает, как выйти из сложившейся ситуации, какие действия и в какой последовательности необходимо произвести, чтобы выйти из ситуации без потерь. То есть знания проблем, возникающих при работе в Интернете, является недостаточным, необходимо иметь алгоритмы поведения в сложных ситуациях, возникающих в информационном пространстве. Следует отметить, что более младшее поколение

гораздо лучше владеет средствами защиты информации. Наши коллеги-историки во время опроса учителей гуманитарного профиля провели опросы и обсуждение информационных войн как в прошлом, так и в настоящее время, и обратили внимание на существенные изменения методов их проведения, вызванные современным состоянием информационных технологий. Заметим, что все опрошенные нами имеют достаточно полное представление об информационных войнах.

Третий круг вопросов был связан с работой в социальных сетях.

Социальными сетями пользуются практически все, часто используемые сети – «ВКонтакте», на втором месте «Instagram» и на третьем «Одноклассники». Также хочется отметить, что как подростки, так и более старшее поколение при работе в данных сетях вводят свои персональные данные. При этом уровень доверия социальным сетям гораздо выше, чем уровень доверия официальной прессе и телевидению.

В процессе работы по изучению уровня знаний людей с педагогическим образованием в области информационной безопасности мы пришли к выводу, что необходимо организовать их обучение в рамках специальных курсов и включить в этот курс следующие модули:

1. Нормативно-правовой модуль, содержащий те законы, которые применяются и используются в обыденной жизни в современном информационном обществе, с примерами их применения.

2. Административный модуль, отражающий правила и нормы поведения гражданина во время работы в организации или учреждении с современными информационными системами.

3. Программно-технический модуль, в рамках которого необходимо ознакомить обучаемых с современными программно-техническими средствами, обеспечивающими информационную безопасность пользователя.

Список литературы

1. Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных».

3. Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 №438-ФЗ (ред. от 29.06.2015).

4. Галатенко В.А. Основы информационной безопасности [Текст] / В.А. Галатенко. – М.: ИНТУИТ.РУ, 2003. – 211 с.

5. Минаев В.А. Правовое обеспечение информационной безопасности [Текст]: учебник / В.А. Минаев [и др.]. – 2-изд., доп. – М.: Маросейка, 2008. – 368 с.

6. Привалов А.Н. Основные угрозы информационной безопасности субъектов образовательного процесса / А.Н. Привалов, Ю.И. Богатырева // Известия ТулГУ. Серия: Гуманитарные науки. – 2012. – Вып. 3. – С. 427–431.

7. Тимошенко В.Н. Вакцинация от фальсификации / В.Н. Тимошенко, М.И. Романова, В.А. Казинец [и др.]. – Хабаровск, 2016. – 95 с.