ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СЕТИ ИНТЕРНЕТ: ПРОБЛЕМЫ И ПУТИ РЕШЕНИЯ

Сборник материалов

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

СТЕРЛИТАМАКСКИЙ ФИЛИАЛ
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО
ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ
ВЫСШЕГО ОБРАЗОВАНИЯ
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

КОЛЛЕДЖ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СЕТИ ИНТЕРНЕТ: ПРОБЛЕМЫ И ПУТИ РЕШЕНИЯ

Сборник материалов

I Республиканской научно-практической конференции школьников 9–11 классов и студентов учреждений среднего профессионального образования

г. Стерлитамак, Республика Башкортостан, 25 февраля 2017 г.

Стерлитамак 2017

УДК 334:342.9(061.3)
ББК 65.29.4+67.401.114я431
И 74

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СЕТИ ИНТЕРНЕТ: ПРОБЛЕМЫ И ПУТИ РЕШЕНИЯ: Сб. материалов I Республ. науч.-практ. конф. школьников 9–11 кл. и студентов учреждений среднего профессионального образования, г. Стерлитамак, Республика Башкортостан, 25 февраля 2017 г. / Отв. ред. Н. Н. Ткачева. – Стерлитамак: Стерлитамакский филиал БашГУ, 2017. – 107 с.

И 74

В сборнике представлены материалы I Республиканской научно-практической конференции «Информационная безопасность в сети интернет: проблемы и пути решения».

Сборник адресован преподавателям и студентам средних профессиональных образовательных учреждений.

СОДЕРЖАНИЕ

Белобородова Т. Г.
Стерлитамакский филиал
ФГБОУ ВО «Башкирский государственный университет»
Республика Башкортостан, г. Стерлитамак

ДИСТАНЦИОННЫЕ ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ В ШКОЛЕ

Сегодня традиционные образовательные технологии перестали полностью обеспечивать потребности динамично развивающегося общества. Растет количество информации, так необходимое для получения, понимания и усвоения начального, основного и среднего (полного) уровней образования. К обучению предъявляются новые требования, такие как непрерывность, мобильность, гибкость, доступность.

Обычная школа в рамках классно-урочной системы сегодня уже не может дополнительно расширить образовательную деятельность для каждого учащегося. Поэтому каждый родитель, видя стремление к учебе своего ребенка (а иногда и при отсутствии этого), старается дополнительно «отдать» ученика в другие образовательные учреждения или на занятия в рамках «репетиторства».

Наряду с этим современное оснащение муниципальных образовательных учреждений материально-техническими средствами позволяет без особых затрат увеличить время пребывания ребенка в образовательном процессе за счет его частичной виртуализации или ускорить этот образовательный процесс. Достигнуть этого позволяют новые информационно-коммуникационные технологии.

В одной из публикаций, журнал Forbes, говоря о технологиях в образовании, называет пять главных трендов: дистанционное обучение, персонализация, геймификация, интерактивные учебники, обучение через видеоигры.

Под дистанционными образовательными технологиями будем понимать образовательные технологии, реализуемые в основном с применением информационных и телекоммуникационных технологий при опосредованном (на расстоянии) или не полностью опосредованном взаимодействии обучающегося и педагогического работника.

Наряду со сказанным выше, еще одним аргументом в пользу использования дистанционных образовательных технологий в обучении является то, что дистанционные образовательные технологии являются частью приоритетного национального проекта «Образование» по направлению «Информатизация образования».

Процесс информатизации системы образования сегодня предполагает:

- введение информационных ресурсов и технологий в учебный процесс и в организацию внеучебной деятельности;
- введение информационных технологий в процесс управления на всех уровнях системы образования;
- введение механизмов поддержания актуальности информационных ресурсов.

Для централизованного управления «виртуальным образовательным процессом» используют системы дистанционного обучения (СДО). Эти системы не отменяют тра-

дицонную классно-урочную систему, а лишь дополняют её. Примером может быть консультирование по предметам, которое преобладает при обучении дистанционно.

В существующем сегодня подходе к организации учебного процесса, использование дистанционных приемов обучения должно носить системный характер, который охватывает сразу несколько направлений деятельности.

Дистанционное обучение привнесёт в жизнь школы много нового:

- саму систему дистанционного обучения (например, LMS Moodle, Прометей, E-learning, и т.д.);
- хранилище данных с поиском, совместным доступом к документам и возможностью их публикации в Интернет (например, на базе сервиса GoogleDocs);
- средства дополнительного контроля успеваемости учеников (например, на базе LMS Moodle);
- почтовую систему с персонально настроенными анти-спам фильтрами.

Одна из самых сильных сторон системы дистанционной подготовки школы − это широкие возможности для коммуникации. Система поддерживает обмен файлами любых форматов – как между преподавателем и учащимися, так и между самими учащимися. Сервис рассылки позволяет оперативно информировать всех участников курса или отдельные группы о текущих событиях.

Что такое электронное обучение?

Главными целями использования ДОТ в школе являются:

- ликвидация разрыва между образовательными потребностями обучающихся и возможностями образовательного учреждения удовлетворить данные потребности;
- повышение качества образования одаренных обучающихся в соответствии с их интересами и способностями, обучающихся-детей с ограниченными возможностями здоровья;
- ликвидация вакансий педагогических кадров за счет использования ДОТ.

Работа со школьниками имеет особую специфику. Ведь школьники не могут в полной мере сами планировать свой образовательный процесс, есть проблемы с доступом к цифровым ресурсам в определённых моделях обучения. Стоит принять во внимание еще и то, что дистанционное обучение предполагает преобладание самостоятельной работы. Поэтому необходимо учесть, что обучающийся должен обладать навыками самостоятельной работы и что контроль будет осуществляться в основном в тестовой форме.

Основные направления использования ДОТ в школе:

1. Дистанционная поддержка образования детей с ограниченными возможностями здоровья:
   - расширение контингента учащихся;
   - реализация программ дополнительного образования;
   - организация обучения по общеобразовательным программам.
2. Дистанционная поддержка образования одаренных детей:
   - заочные туры олимпиад;
   - выполнение проектов и исследовательских работ;
   - дистанционные факультативы по различным предметам;
   - дистанционные консультации;
   - дистанционные викторины, конкурсы.

3. Профильное обучение с использованием дистанционных образовательных технологий.

4. Организация дистанционного контроля знаний учащихся.

5. Организация дополнительных элективных курсов.

6. Экстернат.

7. Уроки с использованием дистанционных образовательных технологий для пропускающих школьные занятия детей по причинам болезни.

8. Повышение квалификации учителей.

В последнее время все более широко в школах, в 10–11 классах получает распространение обучение по индивидуальным программам. Становится все более очевидным тот факт, что классно-урочная система, существующая так давно, тормозит интеллектуальное развитие ученика старших классов. Проведение 6–7 уроков по 45 минут, в течение которых ученик должен вникнуть в суть нового знания, а затем выполнение домашних заданий не оставляют никаких шансов для углубленного изучения предмета, более серьезного исследования проблемы, самостоятельного поиска информации для решения этой проблемы. А ведь формирование умений работать с информацией – это одна из главных целей современного образования. Совершенно спокойно можно большую часть информационного материала перенести на дистанционные формы, включая и возможные формы тестирования, контроля и необходимых консультаций. Частичная замена классно-урочной деятельности на самостоятельные виды деятельности не только значительно разгружает столь драгоценное дневное время ученика, но и создает условия для продуктивной самостоятельной творческой деятельности, а учителю дает возможность дополнительных консультаций тем учащихся, которые в этом нуждаются.

Например, в программе дистанционного обучения английскому языку должны присутствовать несколько функций, которые обеспечивают ее интерактивность:

- уроки-чаты с преподавателем и другими учащимися школы;
- форум, где можно обсудить различные актуальные темы, в том числе и носителями языка;
- переписка по электронной почте с учителем, одноклассниками и носителями языка;
- наличие разнообразных творческих заданий, требующих не только углубленных знаний по предмету, но и творческих способностей учащихся;
- систематическая организация различных конкурсов и олимпиад;
- проверка письменных и устных заданий учителем в режиме on-line;
- встроенный в программу дистанционного обучения табель успеваемости на основе балльно-рейтинговой системы оценивания, позволяющий учащимся корректировать свой индивидуальный темп обучения.

Дистанционное обучение решает проблемы, когда возникают трудности с качественным обеспечением учащихся очными формами обучения. Это дети-инвалиды, для которых посещение очной системы обучения вызывает затруднения, а также одаренные дети сельской местности, желающие повысить свой уровень знаний.

Как уже отмечалось выше, дистанционные технологии – это инструмент для реализации принципов личностно-ориентированного подхода обучения. Система преду-

сматривает постоянное общение обучающихся как между собой, так и с преподавателем. Но это должно быть сотрудничеством, а не передачей знаний.

К плюсам дистанционных образовательных технологий можно отнести:

- Обучение в индивидуальном темпе – скорость изучения устанавливается самим обучающимся в зависимости от его личных обстоятельств и потребностей.
- Свобода и гибкость – обучающийся может выбрать любой из многочисленных курсов обучения, а также самостоятельно планировать время, место и продолжительность занятий.
- Доступность – независимость от географического и временного положения обучающегося и образовательного учреждения позволяет не ограничивать себя в образовательных потребностях.
- Мобильность – эффективная реализация обратной связи между преподавателем и обучаемым является одним из основных требований и оснований успешности процесса обучения.
- Технологичность – использование в образовательном процессе новейших достижений информационных и телекоммуникационных технологий.
- Социальное равноправие – равные возможности получения образования независимо от места проживания, состояния здоровья, элитарности и материальной обеспеченности обучаемого.
- Творчество – комфортные условия для творческого самовыражения обучаемого.
- Объективность – в результате использования интерактивных практикумов, различных форм тестирования оценка знаний может проходить в автоматическом режиме, без участия преподавателя. Это исключает предвзятость.

Можно назвать ещё множество плюсов использования дистанционных образовательных технологий в учебном процессе школы, они не заменяют обычные занятия в классе и не умаляют роли учителя, а могут очень эффективно дополнить их.

Подводя итог можно предположить, что при «умной» и осмысленной организации использования ДОТ можно добиться не только положительных результатов обучения, но и в ряде случаев решить острые проблемы организации учебного процесса.

Обучение с использованием ДОТ может осуществляться как по отдельным предметам и курсам, включенным в учебный план образовательного учреждения, так и по всему комплексу предметов учебного плана.

Как же построены все системы дистанционного обучения? Естественно на основных принципах современного Интернета, сочетаний веб-технологий, видеосвязи, электронной почты. Итак, для дистанционного обучения нужны:

- Интернет с нормальной скоростью и ПК с веб-камерой.
- Программные средства для видеосвязи – например, скайп (Skype) на ПК учителя и учеников.
- Специализированный сайт с обучающими курсами, на который вы переходите, как правило, по ссылке с сайта школы дистанционного обучения. Для размещения средств дистанционного обучения наиболее подходит система управления обучением Moodle.

Как это работает? Ученики сидят перед компьютерами дома, учитель – на рабочем месте, либо тоже дома. Общение может осуществляться посредством видеосвязи, например, через скайп. На этом уровне может происходить объяснение материа-

ла, и ученик может получать ответы на вопросы. «А как же объяснять без доски и мела?» – спросите вы. Это не проблема, учитель показывает ученикам свой рабочий стол, запускает программу для рисования (любое средство, облегчающее объяснение, презентацию, видеоролик) и рисует с помощью мышки или графического планшета точно так же, как на обычной школьной доске.

Задания могут решаться как в специальных тетрадях, так и на личной страничке, открытой в веб-браузере на компьютере у ученика. Личная страничка отображает содержимое веб-сайта, например, созданного в специальной системе управления обучением Moodle. На этой страничке ученик, зарегистрированный пользователь, может выбрать предмет обучения, посмотреть задания, отправить их на проверку, посмотреть вспомогательные материалы и т.д. В свою очередь, этот веб-сайт размещается точно так же как и миллионы обычных веб-сайтов Интернета, на сервере, специально выделенном или виртуальном хостинге. Соответственно, учитель имеет свой уровень доступа к системе и имеет несколько более широкие возможности, по сравнению с учениками. Может создавать и корректировать содержимое учебных курсов, просматривать задания и т.д. Тестовые задания, как правило, проверяются сразу в автоматическом режиме. А результаты учебы заносятся программой и преподавателем в электронный журнал. Работоспособность всей системы дистанционного обучения поддерживает специально выделенный администратор, но это, конечно, в первую очередь проблема школы. Ответственность за работоспособность клиентской части, той, что у ученика дома, ложится на родителей. Вот самые общие принципы работы системы дистанционного обучения.

Для построения дистанционного обучения необходимо внедрение системы дистанционного обучения (оболочки, платформы), которая обеспечит предоставление необходимых для организации и проведения обучения сервисов. Современные системы дистанционного обучения обеспечивают дистанционные курсы.

Основным средством (не всегда обязательным), используемым при проведении дистанционного обучения, является дистанционный курс, работая с которым учащиеся получают знания и приобретают необходимые им навыки и умения. Остальные средства, используемые в дистанционном обучении, обычно применяются совместно с дистанционными курсами.

Дистанционный курс может содержать большой диапазон элементов:

- информационные слайды;
- симуляции работы с программным обеспечением;
- интерактивные тренажеры;
- тесты;
- ролевые упражнения и т.д.

Помимо различных элементов, включаемых в дистанционный курс с целью предоставления обучаемым знаний, а также развития необходимых им навыков и умений, дистанционный курс включает информацию, как с его помощью должно проводиться дистанционное обучение. В большинстве случаев дистанционный курс включает в себя правила, определяющие, как слушатель переходит от раздела к разделу дистанционного курса при прохождении дистанционного обучения. Перечень таких правил называют траекторией дистанционного обучения.

Важнейшей задачей, стоящей при проведении дистанционного обучения, является организация взаимодействия между учащимися и преподавателями. Существует большой набор средств, которые могут быть использованы для решения этой задачи.

Наиболее широкое распространение получили следующие:

- электронная почта;
- чат;
- форум;
- блог;
- видео- и аудиоконференции.

Аудио- и видеоконференции часто используются при проведении семинаров, на которых освещаются небольшие отдельные темы. Такие семинары крайне эффективны при использовании их для обучения хорошо подготовленных специалистов, для которых необходимо осветить новый или вызывающий у них затруднение вопрос.

Сейчас все большую популярность при построении дистанционного обучения получают инструменты Web 2.0. Особенностью Web 2.0 является принцип привлечения пользователей к наполнению и многократной выверке контента. Примером является всемирная виртуальная энциклопедия – Википедия. Применение технологий Web 2.0 может быть довольно разнообразным. Например, слушатели дистанционного обучения могут совместно выполнять задания. В этом случае итоговая оценка выставляется на основании измерения активности слушателя.

Разобрав основные принципы удаленного обучения, рассмотрим реально существующие примеры школ, реализующих полностью или частично эту идею.

НП «Телешкола», веб сайт http://www.internet-school.ru/teleschool/.

Существует достаточно давно, с 2000 года. Работа организованна на основе образовательной платформы «Интернет-школа «Просвещение». Эта платформа используется как для полностью дистанционного обучения, так и для частичного онлайн обучения, путем использования учебных электронных ресурсов для обычных школ.

Обучение детей (учащихся) происходит как на базовом, так и на профильном уровне. В данной школе реализуют идеологию образовательных сетей, путем объединения образовательных ресурсов, преподавателей и тьюторов (преподавателей консультантов) разных общеобразовательных учреждений. В НП «Телешкола» можно обучаться с 1 по 11 классы. Школа является учреждением дающим полноценное среднее образование дистанционно. Так, в ней можно помимо полного дистанционного обучения, пройти удаленные курсы по какому-либо предмету, либо пройти курсы по подготовке к ЕГЭ. Есть экстернат, но только с 5 по 11 классы. Есть возможность проведения учениками 10–11 классов интегративных опытов по химии, физике и биологии.

Рассмотрим, что представляет собой интернет-урок в данной школе. Интернет-урок включает в себя учебный материал, сопровождающийся картинками, схемами, графиками, картами и т.д. Для изучения данного материала требуется от 1 до 5 часов, в зависимости от урока. Так же в Интернет-уроке содержится домашнее задание, по одному или нескольким вариантам. Кроме того, в Интернет-уроке есть тестовые задания для проверки понимания учениками темы Интернет-урока. Тесты проверяются автоматически, а их результаты публикуются сразу. Тест можно выполнить не-

сколько раз, но с каждым последующим ответом на тест, отметка автоматически снижается. Помимо тестов есть задания с открытым ответом – ученики пишут ответ в специальное поле для ответа, такие задания проверяются учителем. Ну и, конечно, в том случае, если возникают трудности в понимании материала, ученик консультируется с учителем.

Государственное бюджетное общеобразовательное учреждение города Москвы Центр образования «Технологии обучения», а чаще её зовут именно «i-Школа» http://iclass.home-edu.ru/ строит свою работу на системе дистанционного обучения LMS Moodle. «i-Школа» проводит подготовку по инклюзивному образованию, учениками школы становятся дети с ограниченными возможностями и дети, которые вынуждены много времени проводить в больнице. Для них используются самые передовые технологии обучения на базе информационно-коммуникационных технологий. Формы обучения в школе – дистанционная и очно-дистанционная.

Дистанционное образование и электронное обучение положили начало новому общемировому явлению – smart education (умное образование). И речь уже идет не столько о технологиях, сколько о новой философии образования.

В XXI веке технологии стали умными (smart), они делают нашу жизнь комфортнее, безопаснее, разнообразнее, интереснее и настолько проникают во все сферы деятельности, что меняется парадигма общественного развития от информационной к smart-обществу.

Интернет размывает границы экономики, общества и индустрий, изменяя правила игры, открывая вероятность для риска, также как новые возможности. Smart – это свойство объекта, характеризующее интеграцию в данном объекте двух или более элементов, ранее не соединяемых, которая осуществляется с использованием Интернет. Например, Smart-TV, Smart-Home, Smart-Phone. Smart-технологии приведут к расширению трудовой мобильности: в образовании, в государственной службе и во многих других сферах занятости.

Подготовить специалиста, обладающего навыками работы в Smart-обществе, – задача Smart-университета.

Концепция Smart-образования – гибкость, предполагающая наличие большого количества источников, максимальное разнообразие мультимедиа (аудио, видео, графика), способность быстро и просто настраивается под уровень и потребности слушателя. Помимо этого, Smart-образование должно быть легко управляемым, когда учебное заведение может легко обеспечивать гибкость учебного процесса, и интегрированным, то есть постоянно питающимся внешними источниками.

Согласно концепции Smart-образования, новые характеристики приобретает современный учебный курс.

Он должен обеспечить одновременно и качество образования, и мотивировать студента к изучению. Заинтересовать современного студента, имеющего доступ к многочисленным электронным материалам, простым текстовым пособиям практически невозможно. Необходимо создание сценария всех учебных мероприятий курса, которые будут увлекать студента, побуждать его к творческой и научной деятельности. Учебные курсы должны быть интегрированными, то есть включать в себя и мультимедийные фрагменты и внешние электронные ресурсы. Smart-курс должен на 80 % состоять из внешних источников, развиваться самостоятельно за счет подклю-

чений к различным каналам, позволять студенту создавать контент. Современный курс – это траектория действий, среди которых чтение учебника занимает не более 20–30 % времени.

В Республике Башкортостан именно смарт-образование (smart education), базирующееся на электронном обучении (e-Learning), было выбрано в качестве приоритетного направления до 2022 года.

Икрамов Р. Д.
Стерлитамакский филиал
ФГБОУ ВО «Башкирский государственный университет»
Республика Башкортостан, г. Стерлитамак

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: МИРОВАЯ ПРАКТИКА

В связи с постепенной компьютеризацией населения планеты, снижения стоимости производства персональных компьютеров и носимой техники, постепенно растет роль, как самих информационных технологий, так и информационной безопасности. Даже самые консервативные люди постепенно начинают осваивать для себя невиданные до сегодняшнего дня технологии. Трудно представить, но вся компьютерная мощь планеты 1970–1980 гг. может уместиться теперь в форму обычных наручных часов. Подобное развитие технологий постепенно меняет и отношение общества к нему: от неприязни до полной зависимости.

Если Интернет-аддикцию у человека можно считать болезнью XXI века, то финансовые компании, банки и просто небольшие фирмы зависимы от компьютеров и Интернета уже давно. Бухгалтерская отчетность, сводки, справки теперь сдаются онлайн, минуя бесконечные очереди в налоговых органах.

Столь важные операции, как, например, сдача налоговой декларации, заставляют ломать голову многих специалистов: «А как сделать подобную технологию безопасной?». Такой же вопрос задают и специалисты, создающие новые устройства или улучшающие имеющиеся.

Не дают покоя вопросы безопасности, конечно же, в первую очередь государству. Компьютеризация населения позволяет, не выходя из дома, путешествовать по всему миру, смотреть достопримечательности, получать такую информацию, о которой люди и не мечтали 20 лет назад. Если люди старшего возраста заходят в Интернет получить интересующую их информацию, то младшее поколение в основном проводит в Интернете огромное количество времени для расслабления или от безделья, а иногда и от зависимости. Так как нет строгого возрастного и родительского контроля, подростки могут получать как нежелательную, так и запрещенную информацию, что порождает большое количество социальных и политических проблем. Интернет также могут использовать различные террористические, экстремистские и религиозные организации для вербовки, «промывки мозгов» и других, в том числе политических, целей [1, с. 30].

Данная причина сыграла роль в создании проекта PRISM Соединенными Штатами Америки. PRISM – комплекс административных и технологических решений, направленных на сбор и анализ электронно-цифровой информации, аудио-, видео файлов и др. Данный проект создавался секретно ЦРУ и АНБ США, пока в 2013 году сотрудник этих спецслужб Эдвард Сноуден [2, с. 763] не раскрыл правду касаемо этого проекта. Правительство США подтвердило существование данной системы, но уточнило, что она не нарушает законодательства. К проекту подключены крупнейшие компании, такие как Microsoft, Google, Facebook, Apple.

Сноуден утверждает, что спецслужбы США собирают информацию буквально о каждом пользователе Интернета, включая данные с микрофонов и веб-камер, встроенных в ноутбуки, электронную почту. Данная информация может использоваться как для предотвращения различных терактов, так и для шантажа, если собирается информация о высокопоставленном лице.

Стоит ли нарушать право на частную жизнь в обмен на национальную безопасность – вопрос спорный.

Стоит отметить, что США неоднократно выступала в ООН с различными предложениями и заявлениями касаемо информационной безопасности. Так, например, вместе с Австралией был создан союз по совместной защите от кибератак.

Внутреннюю политику США в сфере информационных технологий можно считать одной из самых продвинутых. На развитие IT-технологий тратится около 100 миллиарда долларов ежегодно. Поэтому в США сильно развита робототехника, беспилотные летательные аппараты, необитаемые подводные аппараты. Существуют программы, по которым учащимся информационных вузов оплачивает проживание в общежитии, обучение и книги. Крупных специалистов, выдающихся мошенников и хакеров приглашают на работу в государственные органы в качестве консультантов.

В Китае на настоящий момент совсем другой к подход к безопасности в сфере информационных технологий. В 2003 году запущен проект «Золотой щит» [3, с. 95], который нередко называют «Великий китайский файервол». «Золотой щит» представляет собой огромную систему для фильтрации Интернет-траффика. Стоимость проекта около 800 миллионов долларов. Руку приложили крупнейшие мировые компании, в том числе IBM.

«Золотой щит» анализирует Интернет-траффик, поисковые запросы, веб-сайты на предмет неугодных коммунистической партии или китайскому законодательству материалов. На ресурсах запрещены такие слова как «демократия», «свобода слова», «контрреволюционный», «митинги», «репрессии» и многие другие. Если пользователь введет поиск одно из этих слов, то появится «окошко», которое уведомит пользователя, что доступ к данному ресурсу заблокирован коммунистической цензурой.

Запрещены сайты, содержащие антикоммунистическую пропаганду, пропаганду свободы слова, критику в адрес правительства страны. При этом не запрещена критика в адрес конкретных чиновников из-за периодически проводимой Китаем антикоррупционной компании.

Помимо автоматической цензуры «Золотой щит» имеет и постмодераторов. Это так называемая «Интернет-полиция» Китая [4, с. 333] – более 1000 человек работают в Интернете, ища ресурсы и материалы, так или иначе запрещенные китайским законодательством.

Многие Интернет-порталы, такие как Facebook, Google, Apple, Microsoft, Wikipedia, Twitter, запрещены, что открывает большие возможности для создания социальных сетей, масс-медиа, предназначенных исключительно для внутреннего рынка, то есть жителей Китая. Так, в Китае есть аналоги видеохостинга Youtube, микроблоггинга Twitter, поисковой системы Google, базы знаний Wikipedia и т.п.

Таким образом, рассмотрено два подхода к обеспечению безопасности страны с помощью информационных технологий. Несмотря на нарушения моральных и этических норм, системы обладают некоторыми достоинствами, если их использовать по прямому назначению: нахождение действительно опасной информации, предупреждение различных террористических атак и нахождение опасных преступников и организаций.

Сложно сказать, какое самое оптимальное решение нужно принять для обеспечения безопасности государства. Возможно, что ответ лежит где-то посередине. Нужно находить действительно опасный материал и анализировать Интернет-траффик, и лишь в самых серьезных случаях принимать какие-либо действия. Школьник, скачивающие нелицензионные компьютерные игры, или студент, изучающие не самые приятные моменты истории страны, не являются серьезной угрозой целостности государства, как взрослый человек, вербующий подростков с неокрепшей психикой. Данным анализом и должно заниматься государство, скрытно и незаметно, не нарушая покоя населения.

Список литературы

1. Жаворонкова Т. В. Использование сети интернет террористическими и экстремистскими организациями // Вестник Оренбургского государственного университета. – 2015. – № 3. – С. 30–36.

2. Букреева Т. Н. Отражение международной ситуации в языке средств массовой информации (на примере китайского языка) // Молодой ученый. – 2015. – № 11. – С. 763–765.

3. Лексютина Я. В. Свобода интернета в современном дискурсе американо-китайских отношений // Социально-экономические явления и процессы. – 2011. – № 11. – С. 95–98.

4. Шебуняева Е. А., Локотков А. А. Особенности внедрения информационных технологий: зарубежный опыт // Молодой ученый. – 2011. – № 3–4. – С. 333–342.

Баймурзина А. А.
Научный руководитель – учитель информатики
Нигматуллин Х. Х.
МБОУ «Башкирская гимназия № 25»
Республика Башкортостан, г. Салават

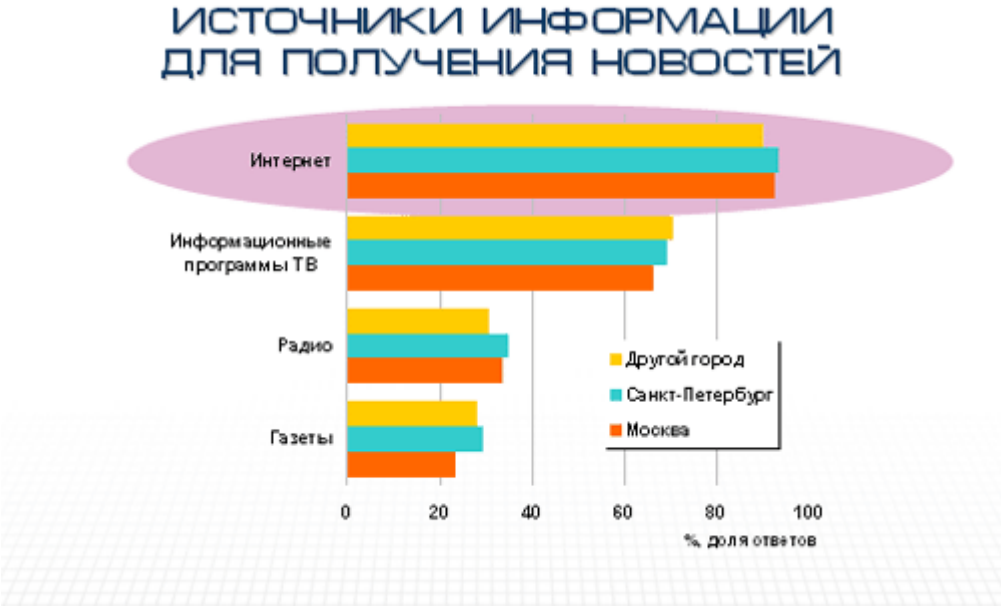
ИНТЕРНЕТ-ФАКТОР В ЦЕННОСТНОМ РАЗВИТИИ МОЛОДЕЖИ РОССИИ

Интернет в современном мире становится важным фактором влияния на систему ценностей молодежи и формирования экстремистских установок. На сегодняшний день проблема заключается в том, что социализация молодежи проходит под влиянием Интернета, социальных сетей. Современная молодежь, можно сказать, поглощается просторами Интернета.

Средства массовой информации в современном информационном обществе взяли на себя значительную часть функций по формированию сознания людей: воспитанию их вкусов, привычек, предпочтений.

Молодое поколение начинает зависеть от Интернета, доверяясь его модным тенденциям. Прилагает максимум усилий для их достижения. И не важно, чем он ради этого ограничиться: прогулки с друзьями, общения с родителями. Из чего следует замкнутость индивида, потеря «смысла жизни», неумение ярко выражать свои чувства.

Интернет является основным источником информации для пользователей интернета. Это могут доказать следующие показатели [3]:



Цель работы: выявить факторы, влияющие на ценностное развитие молодежи.

Задачи:

- рассмотреть положительное и отрицательное влияние Интернета;
- выявить изменения ценностных ориентиров современной молодежи под влиянием Интернета.

Хотелось бы вначале рассмотреть положительные стороны «Всемирной паутины». Во-первых, быстрота нахождения нужной информации. Во-вторых, Интернет позволяет заниматься само-PR. Особенно распространенно среди людей, занимающихся творчеством. В-третьих, возможность заниматься самообразованием и обучением. В-четвертых, поддерживание общения с друзьями и родственниками. В-пятых, возможность совершать покупки через Интернет-магазин «не выходя из дома».

Но минусов, нам кажется, все-таки больше. Ведь в процессе работы в Интернете надо не только научиться работать за компьютером или девайсом, но и уметь целенаправленно его использовать для познания и созидания окружающего вас мира. Перечислим некоторые недостатки [6, с. 5]:

- зачастую невозможно подтвердить достоверность информации;
- при неправильном использовании, потеря конфиденциальности;
- Интернет не может заменить настоящего, живого общения;
- Российский сегмент Интернета зачастую способствует пиратству;
- мошенничество;
- зависимость;
- влияние на зрение;
- возбуждение некоторых видов болезни.

Хотелось бы на жизненном опыте рассмотреть положительную и отрицательную сторону Интернета.

Интернет-магазин на сегодняшний день очень актуален. Мы, как и многие пользователи Всемирной паутины, решили заказать одежду с Интернет-магазина, так как там можно приобрести одежду, которую невозможно найти в магазинах нашего города Салават. Нашли понравившуюся вещь, прочитали описание к ней (оно было довольно заманчивым) и решились ее приобрести. Оплатили товар через Киви-кошелек, внесли адрес доставки. В общем, сделали все, что требовалось по инструкции, предоставленной Интернет-магазином. Теперь дело стояло за продавцом. Товар, как было написано в описании, должен был прийти за 15–20 дней. Прошел месяц, но свою одежду мы так и не получили. Связавшись с продавцом, получили информацию, что надо подождать еще некоторое время, на что мы согласились. Прошел еще месяц, а мы так и не получили свою посылку. Еще раз связались с продавцом, настояли на возврате денежных средств. С этим, к счастью, проблем не возникло. Деньги перевели на счет примерно через 1–2 дня.

Общее впечатление от первого заказа, у нас конечно, не очень хорошее. Но, нам кажется, не все Интернет-магазины и покупатели встречаются с подобной проблемой. Для себя мы сделали такой вывод: решаясь приобрести какой-либо товар, нужно помнить, что ты рискуешь своими денежными средствами, временем, нервами. Есть случаи, когда покупатель не получает свой товар, при этом не возвращается и оплата за неполученную покупку. Нужно подробно узнать в Интернете все подробности и прочитать комментарии покупателей, по возможности проконсультироваться на форуме или онлайн-помощником, если такая функция имеется у магазина.

Интернет – всемирная паутина, которая хранит огромное количество информации, за которой просто невозможно уследить. Любой пользователь Интернета может внести что-то «свое», без подтверждения компетентных администраторов. Т.е. в просторы всемирной паутины с легкостью могут попасть вирусы: рекламные про-

граммы, бэкдоры, загрузочные вирусы, макровирусы, фарминг, Bot-сеть, эксплойт, ловушки, ноах; пропаганда против страны и т.п.; распространение сектантских групп и многое другое. А значит, любой ребенок может с легкостью попасть в подобные сайты, где может содержаться «информация», которую по закону должна быть доступна для просмотра только после 18 лет. Ребёнок, посетив такие сайты, может кардинально изменится, причем не в хорошую сторону. Информацию, которую он получит на запрещенных сайтах, может опробоваться ребенком в реальной жизни. А ведь именно то, что закладывается в нас в детстве, является фундаментом нашего дальнейшего развития. Так какое же молодое поколение последует далее? Какие будут у них вкусы и цели в жизни?

На сегодняшний день, современная молодежь сильно отличается от молодежи, хотя бы 90–2000-х годов. Каких-то только 15–20 лет назад, молодое поколение больше посещало культурные мероприятия: кино, музеи, выставку картин и скульптур, и т.п. Больше радовалось маленьким мелочам, хотя бы пролетевшей мимо бабочки. Сегодня же, молодое поколение больше предпочитает уделять время для самосовершенствования своей «внешней оболочки», вовсе забывая о «внутренней». Ведь социальные сети в большей степени заполнены группами, страницами, где рекламируются «эталоны красоты», за которыми многие из нас и следуют. Конечно, это не есть плохо, но для чего быть красивым снаружи, если внутри ты «пуст».

Как говорилось ранее, Интернет в современном мире становится важным фактором влияния на систему ценностей молодежи. Следовательно, только Интернет может помочь нам в решении такой проблемы как, изменения системы ценностей молодежи. Каким же образом?

«Ценности, – писал В. П. Тугаринов, – это то, что нужно людям для удовлетворения потребностей и интересов, а также идеи и их побуждения в качестве нормы, цели и идеала» [4].

Аристотель, например, считал, что человеческая жизнь – это высшая ценность, которая превосходит все другие ценности, а цель и смысл человеческой жизни – разумная деятельность, направленная на достижение поставленных целей; высшая цель человека – достижение счастья (блага, «арете»), сущность которого – умение человека выявить и проявить в своей деятельности и общении с другими людьми свою функциональную значимость для социальной общности, в которой он живет (семья, община, полис), и свои моральные достоинства (мужество, бескорыстие, великодушие и др.); высшая ступень счастья – созерцание (занятие философией) [5].

Ценности могут усваиваться осознанно и неосознанно. В последнем случае, человек не всегда может понять и объяснить, почему отдает предпочтение тем или иным ценностям. Они сегодня активно внедряются в сознание при помощи средств массовой информации. При формировании собственной системы ценностей, молодые люди ориентируются не только на общественную систему, но и на выбранные ими самими образцы для подражания. При всем при этом сейчас идет разрушение системы воспитания – сегодня воспитывают главным образом семья, улица, телевидение, поэтому необходимо заниматься проблемой воспитания [1, с. 3].

От ценностных ориентиров молодежи зависит дальнейшее развитие не только нашей страны, но и других стран мира. Поэтому важно понимать, что оно имеет ог-

ромное значение в развитии нашей жизни, и нужно серьезно подходить к решению этой задачи.

Неоднократно повторялось, что СМИ ведет формирование и внедрение ценностных ориентиров в наше сознание. Пользуясь этим же «оружием», можно заниматься и проблемой воспитания молодежи. Для этого вести максимальное распространение: 1) «золотого правила нравственности»; 2) соблюдение этики; 3) оказания помощи людям пожилого возраста; 4) «старших уважай, но и про младших не забывай».

Несколько таких правил вполне хватит для воспитания молодежи, и не только. Они помогут поменять ориентации молодого поколения, впоследствии создав «единый народ», как раньше. Когда помощь окружающим считалась долгом каждого, нежели думать только о себе. В мире, где «каждый сам за себя» вряд ли будет царствовать счастливая жизнь. А зачем нам жить, зарабатывая только на свое материальное благо, если твой народ живет в нищете? Возможно, только мы думаем подобным образом, но, для расцветания нашей страны нужно, чтобы каждый поддерживал это мнение, да бы в равной степени приносить ей только пользу.

После старого поколения, всегда приходит новое, от которого будет и зависеть наша жизнь.

Список литературы

1. Примерные программы по учебным предметам. Информатика и ИКТ. 7–9 классы: проект. – М.: Просвещение, 2010.

2. Семакин И., Залогова Л., Русаков С., Шестаковой Л. Информатика – базовый курс. 9 класс. – 2015.

3. Оптимизация рекламной деятельности ООО «Геолого-разведывательное предприятие поиск. URL: http://refleader.ru/jgebewpolotrqas.html (дата обращения: 18.02.2017).

4. Ценности и их роль в жизни человека [Раздел: Рефераты по социологии]. URL: http://www.bestreferat.ru/referat-162149.html (дата обращения: 18.02.2017).

5. Профессионально-этические основы социальной работы: учебное пособие. Автор/создатель: Махова Н. П., Филатов В. А. URL: http://window.edu.ru/catalog/pdf2txt/266/62266/32196?p_page=3 (дата обращения: 18.02.2017).

6. Макарова Н. В. Информатика. 7–9 класс. Базовый курс. Теория. Под редакцией Н.В. Макаровой. – Питер, 2007.

Беремец А. Ю.
Научный руководитель – преподаватель юридических дисциплин
Голубничий А. С.
Колледж Стерлитамакского филиала
ФГБОУ ВО «Башкирский государственный университет»
Республика Башкортостан, г. Стерлитамак

«ПАКЕТ ЯРОВОЙ» – КАК НОВЫЙ ШАГ К ПРАВОВОМУ РЕГУЛИРОВАНИЮ СЕТИ ИНТЕРНЕТ ИЛИ БАРЬЕР ДЛЯ ИННОВАЦИОННОГО РАЗВИТИЯ

Для того чтобы начать освещать данную тему, необходимо отметить, что на данный момент Интернет «проник» в каждую сферу общественной жизни. Любая работа, услуга осуществляется через персональный компьютер. Использование локальной сети значительно упрощает нашу жизнь, но, не смотря на все ее достоинства, у нее есть «обратная сторона медали». Движения терроризма, детская порнография, призыв к суициду – вот она, черная сторона локальной сети. Каждое государство хочет защитить свой народ от таких призывов и создает для этого специальные программы, которые охраняют нас от них. Например, «Пакет Яровой», созданный в Российской Федерации о котором речь пойдет чуть дальше.

«Пакет Яровой» является новшеством в российском законодательстве. Он представляет собой два законопроекта, имеющие антитеррористическую направленность. Пакет состоит из двух федеральных законов:

1. Федеральный закон от 6 июля № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности».

2. Федеральный закон от 6 июля №375-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности».

Перечислим новшества, которые были введены этими законопроектами:

1. Закон вводит статью УК (205.6) называется «несообщение о преступлении». По ней будут привлекать к ответственности тех, кто не сообщил правоохранительным органам «о лице/лицах, которые по достоверно известным сведениям готовят, совершают или совершили» преступления некоторых категорий. Закон вводит список из полутора десятков преступлений, о подготовке которых необходимо сообщить компетентным органам: от международного терроризма до вооруженного мятежа, направленного против территориальной целостности России. Наказывается штрафом в размере до ста тысяч рублей или в размере заработной платы или иного дохода, осужденного за период до шести месяцев, либо принудительными работами на срок до одного года, либо лишением свободы на тот же срок. От ответственности по статье освобождаются люди, которые не стали сообщать о подготовке и совершении преступления их супругом или близким родственником.

2. Власти вводят новую категорию не выездных. Права покидать Россию лишатся люди с непогашенной или неснятой судимостью за некоторые виды преступлений. Часть этих статей названа напрямую – по номерам. В основном они касаются преступлений, связанных с терроризмом: теракт, захват заложников и прочие. В этом же списке «насильственный захват или удержание власти», «посягательство на жизнь государственного деятеля», «вооруженный мятеж».

3. Операторов связи и «организаторов распространения информации» в Интернете обяжут хранить на территории России записи звонков («голосовую информацию»), переписку, изображения, звуки, видео и другие сообщения пользователей. Срок хранения – до шести месяцев с момента передачи, приема и/или обработки. Информацию о факте приема или передачи сообщения, или звонков (то есть не содержание, к примеру, переписки, а только сведения о том, что она состоялась) операторы должны будут хранить в течение трех лет. Все эти данные надо будет передавать в правоохранительные органы, если они понадобятся для оперативной работы. Одновременно законопроект вводит в административный кодекс ответственность за использование «несертифицированных средств кодирования (шифрования) при передаче сообщений в информационно-телекоммуникационной сети Интернет». Для юридических лиц – штраф от 30 до 40 тысяч рублей с конфискацией нелегального средства.

4. В статье о свободе совести и вероисповеданий, согласно принятым поправкам, появится определение понятия «миссионерская деятельность». Ею считается религиозная практика вне специальных заведений, кладбищ, мест почитания, религиозных школ – богослужения, церемонии, распространение литературы и других материалов, чтение проповедей. Также миссионерством признаётся «распространение веры и религиозных убеждений» через СМИ и в Интернете. При этом закон предусматривает, что миссионерской деятельностью смогут заниматься только представители зарегистрированных организаций и групп – или люди, которые заключили с ними официальный договор. Каждый миссионер должен иметь при себе документы с определенной информацией, подтверждающие его принадлежность к той или иной организации или группе.

5. В Уголовном кодексе появится новая статья – «Акт международного терроризма». По ней будут судить тех, кого обвинят в совершении теракта за пределами России, в результате которого погибли или пострадали российские граждане, а также тех, кто финансирует подготовку терактов. В качестве наказания статья допускает пожизненный срок лишения свободы.

6. Закон вносит поправку, которая обяжет «операторов почтовой связи» («Почту России» и частные почтовые компании) следить за тем, чтобы в посылках не было ничего запрещенного. В список запрещенного для пересылки входят: деньги, оружие, наркотики, яды, скоропортящиеся продукты и вещества, которые могут навредить сотрудникам почты или повредить другие посылки. Проверять посылки предлагается с помощью рентгена, металлоискателей и других подобных устройств. Сотрудники могут задерживать и даже уничтожать посылки с запрещенными предметами.

7. Закон расширяет список статей, по которым можно судить подростков, достигших 14-летнего возраста. Так им могут вменяться уголовные статьи за:

- международный терроризм;
- участие в террористических сообществах, террористических организациях и незаконных вооруженных формированиях;
- прохождение обучения терроризму;
- участие в массовых беспорядках;

- посягательство на жизнь государственного и общественного деятеля и за нападения на лица и учреждения, которые пользуются международной защитой, а также за угон самолета, поезда или водного транспорта;
- несообщение о преступлении.

На реализацию данного законопроекта необходимы большие затраты. Только после подписания этого закона Президентом выяснилось, что оборудования, необходимого для хранения таких гигантских объёмов данных, нет не только в России, но и во всём мире. В связи с этим В.В. Путин распорядился запустить собственное производство необходимого аппаратного обеспечения. К 1 сентября он также поручил проанализировать возможность, сроки и затраты на организацию производства отечественного оборудования и программного обеспечения, нужного для хранения и обработки данных. Создателями данного пакета являются Яровая и Озеров.

На основе вышесказанного можно сделать следующие **выводы**:

1. Принятие Пакета будет означать вторжение в частную жизнь. Если мы обратимся к Конституции Российской Федерации, то увидим, что статья 23 регламентирует нам, что «каждый имеет право на тайну переписки, телефонных переговоров, почтовых телеграфных и иных сообщений». Следовательно, хранение информации телефонных операторов противоречит Конституции Российской Федерации.

2. Антитеррористический пакет поставит под угрозу национальную безопасность России. Хакеры и иностранные спецслужбы теоретически смогут получить доступ к хранящимся у государства ключам шифрования от защищенных сервисов.

3. Закупка необходимого оборудования увеличит зависимость России от Запада.

4. Россияне могут лишиться доступа к Google.

5. Из-за огромных затрат на аренду серверов и установку оборудования Интернет-компании и сотовые операторы сократят вложения во многие перспективные проекты.

В России практически нет опыта отслеживания зашифрованного трафика мобильных приложений, а тот же Роскомнадзор блокирует сайты только по домену. Более того, для ограничения доступа к защищенным мессенджерам необходимо разработать законодательную базу, которая на сегодня просто-напросто отсутствует.

Но даже если отечественным спецслужбам и удастся ограничить доступ к Telegram и WhatsApp, то террористы наверняка найдут другие способы коммуникации. Например, сеть Tor, взломать которую пока не по силам даже правительству США.

Список литературы

1. «Конституция Российской Федерации» (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ); статья 23.

2. Федеральный закон от 6 июля № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности».

3. Федеральный закон от 6 июля № 375-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности».

Бикбаева Э. И.
Научный руководитель – учитель истории и обществознания
Строчко Т. Н.
МБОУ «СОШ № 24 с углубленным изучением иностранного языка»
Республика Башкортостан, г. Салават

ЗАКОНОДАТЕЛЬНОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИИ

Законодательный уровень является важнейшим для обеспечения информационной безопасности. Большинство людей не совершают противоправных действий не потому, что это технически невозможно, а потому, что это осуждается и/или наказывается обществом, потому, что так поступать не принято.

Актуальность определяется тем, что в современном мире нарастают информационные угрозы. Информационный ресурс в настоящее время выходит по степени значимости на первый план.

Цель правового регулирования информационной безопасности на основе международных соглашений и договоров и нормативно-правовых актов РФ. Для достижения указанной цели поставлены **задачи**:

- рассмотреть информационные основы безопасности;
- изучить источники регулирования информационной безопасности;
- выявить меры по обеспечению информационной безопасности Российской Федерации;
- определить направления совершенствования правового регулирования информационной безопасности.

Самое важное (и, вероятно, самое трудное) на законодательном уровне – создать механизм, позволяющий согласовать процесс разработки законов с реалиями и прогрессом информационных технологий. Законы не могут опережать жизнь, но важно, чтобы отставание не было слишком большим, так как на практике, помимо прочих отрицательных моментов, это ведет к снижению информационной безопасности.

В состав законодательства по обеспечению информационной безопасности включаются федеральные законы, подзаконные нормативные правовые акты федеральных органов исполнительной власти, законы и подзаконные нормативные правовые акты субъектов Российской Федерации.

К числу наиболее значимых нормативных правовых актов в области обеспечения информационной безопасности относятся следующие законы и подзаконные акты.

Конституция Российской Федерации содержит нормы, которые определяют правовые основы информационной безопасности: основные положения правового статуса субъектов информационных отношений, принципы информационной безопасности (законности, уважения прав, баланс интересов личности, общества и государства), конституционный статус государственных органов, обеспечивающих информационную безопасность и др.

Например, к таким положениям относятся нормы, которые устанавливают право каждого субъекта свободно искать, получать, передавать, производить и распространять информацию любым законным способом [1, п. 4. ст. 29].

Это конституционное право, устанавливающее возможность удовлетворения интересов личности и общества сбалансировано необходимостью их ограничения федеральным законом в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства [1, п. 3. ст. 55].

Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности» [2] закрепляет правовые основы обеспечения безопасности личности, общества и государства, определяет систему безопасности и ее функции, устанавливает порядок организации и финансирования органов обеспечения безопасности, а также контроля и надзора за законностью их деятельности.

Закон определяет ключевые термины в области безопасности, которые применимы и для сферы информационной безопасности, принципы и систему безопасности, правовой статус и состав Совета Безопасности Российской Федерации.

Федеральный закон от 27.07.2006 г., № 149-ФЗ «Об информации, информационных технологиях и о защите информации» фиксирует базовые нормы для всей системы информационного законодательства, в т.ч. правового обеспечения информационной безопасности. Они определяют основные термины и их определения, принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации [3, ст. 3], классификацию информации по категориям доступа – общедоступную и ограниченного доступа [3, ст. 5], порядку ее предоставления или распространения (свободно распространяемую, обязательного предоставления или распространения, ограниченного распространения или запрещаемую для распространения вообще). Закон определяет базовые положения правового режима доступа к информации [3, ст. 8] и его ограничения [3, ст. 9], основные параметры правовых режимов распространения [3, ст. 10] и документирования информации [3, ст. 11], информационных систем [3, ст. 13], информационно-телекоммуникационных сетей [3, ст. 15] и общие условия защиты информации [3, ст. 16], информационных систем [3,ст.13] и использования информационных технологий, а также в общих чертах описывает ответственность за правонарушения в сфере информации, информационных технологий и защиты информации.

Сегмент сети Интернет предназначен для обеспечения размещения информации о деятельности администрации Президента РФ, аппарата Совета Федерации, аппарата Государственной Думы, аппарата Правительства РФ, аппаратов Конституционного Суда РФ, Верховного Суда РФ, Высшего Арбитражного Суда РФ, Генеральной прокуратуры РФ и Следственного комитета при прокуратуре РФ, федеральных органов государственной власти и органов государственной власти субъектов РФ, а также для доступа к сети Интернет должностных лиц указанных государственных органов.

В российском правовом пространстве длительное время в обороте используется понятие «служебная информация ограниченного распространения», относимое к деятельности органов государственной власти, которая нередко определяется в нормативных правовых актах как «служебная тайна». Постановлением Правительства РФ от 03.11.1994 № 1233 «Об утверждении Положения о порядке обращения со служебной

информацией ограниченного распространения в федеральных органах государственной власти» [4] определяется правовое положение информации ограниченного доступа, несмотря на то, что согласно п. 1 и 4 ст. 9 Закона «Об информации, информационных технологиях и о защите информации» [5, п. 1 и 4 ст. 9] ограничение доступа к информации и, в частности, отнесение информации к сведениям, составляющим служебную тайну, устанавливается исключительно федеральными законами. Явное несовершенство информационного законодательства и практики его применения отрицательно влияет на состояние правовой защиты интересов субъектов правоотношений. Пробел в нормативных правовых актах, устанавливающих оборот информации служебного характера, не позволяет установить запрет либо ограничения на ее использование, а вместе с этим создает ситуацию невозможности установить административную и/или уголовную ответственность за нарушения порядка распространения этой важной формы информации.

Информационная безопасность является неотъемлемой частью национальной безопасности, в свою очередь, национальная безопасность – это определенная гарантия для жителей государства в сфере обеспечения интересов граждан, национальных приоритетов и образа жизни от всевозможного негативного влияния широкого спектра внутренних и внешних угроз, носящих различных характер (информационный, политический, экологический и проч.).

Мы считаем, что в современном обществе необходимо знание своих прав и законов по обеспечению информационной безопасности. Для достижения поставленной проблемы мы предлагаем следующие **пути её решения**:

- организация дополнительных курсов в школе или во внешкольных учреждениях по изучению данных прав и законов;

- предоставление учащимся возможности изучения прав и законов на уроках информатики;

- создание научно-познавательных сайтов, статей, фильмов по изучению и ознакомлению с правами и законами.

Таким образом, анализ действующего российского законодательства показывает, что вопросы правового регулирования, связанные с функционированием и развитием системы Интернет в России, образуют обширную нормативную базу, включающую только на федеральном уровне более 50 федеральных законов, не говоря уже о многочисленных нормативных правовых актах Президента и Правительства РФ. Спектр этих законодательных актов исключительно широк, и их толкование с позиций специфики правоотношений, возникающих при использовании современных информационных технологий, затруднительно, тем более что при разработке этих законов в них не предусматривались соответствующие возможности. В связи с этим очевидно, что для правоприменительных органов (в том числе для судебных органов) данная область правоотношений является новой.

Список литературы

1. Конституция РФ от 12 декабря 1993 г.

2. Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности».

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

4. Постановление Правительства РФ от 03.11.1994 № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах государственной власти».

5. Федеральный закон «Об информации, информационных технологиях и о защите информации», принят Государственной Думой 8 июля 2006 года.

6. Баранов П. А., Воронцов А. В., Шевченко С. В. Обществознание. Справочник. – 2016. – С. 232.

7. Хорев П. Б., Методы и средства защиты информации в компьютерных системах: Учебное пособие для студентов высших учеб. заведений. – М.: Издательский центр «Академия», 2005. – 256 с.

Волкова М. В.
Научный руководитель – преподаватель экономических дисциплин
Субботина Е. В.
Колледж Стерлитамакского филиала
ФГБОУ ВО «Башкирский государственный университет»
Республика Башкортостан, г. Стерлитамак

ЗАЩИТА ИНФОРМАЦИИ В СФЕРЕ ПРЕДПРИНИМАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТИ

В условиях острой конкурентной борьбы каждая фирма, действующая на рынке, неизбежно сталкивается с необходимостью решения двух проблем.

Первая связана с получением информации о деятельности конкурентов, причем как можно более полной, точной и своевременной. Без наличия такой информации невозможно строить производственную, научно-техническую, финансовую, рыночную стратегии и тактику поведения фирмы. Особенно важна информация, составляющая коммерческую тайну. Зачастую получение такой информации позволяет фирме экономить огромные суммы на научно-исследовательских работах и опытно-конструкторских разработках. Если способы получения информации выходят за разрешенные законом рамки (например, с помощью подкупа сотрудников, незаконного доступа к компьютерной системе), то эта деятельность может считаться коммерческим шпионажем.

Вторая проблема – защита конфиденциальной информации. Как сама фирма стремится узнать секреты других, так и ее конкуренты делают то же самое. Следовательно, каждая фирма может являться одновременно как объектом, так и субъектом коммерческого шпионажа, или, если использовать более «мягкий» термин – экономической разведки.

Объектом преступных посягательств являются люди (персонал фирмы), документы, технические средства, личная переписка сотрудников и даже офисный мусор. По данным исследований, приведенным в отчете компании SecurIT, основными причинами утечек являются: 1) хакерские действия; 2) Интернет сервисы; 3) компьюте-

ры и ноутбуки; 4) мошенничество; 5) мобильные устройства; 6) неправильная утилизация бумажных и электронных носителей; 7) электронная почта и другие.

Согласно последним данным, больше всего утечек регистрируются в трех отраслях розничная торговля (16,2 %), организации здравоохранения (16 %) и госучреждения (15,5 %).

В списке компаний, пострадавших от утечки информации значатся:

1. Компания Apple: у нее в начале 2013 года «угнали» Outlook for Mac. Причем в сети оказалось не только описание, но и наглядное пособие в виде скриншотов, как будет выглядеть новый пакет для макбуков на текущий год. Утечка произошла благодаря китайским ресурсам.

2. Пользователи Google в том же году пострадали от утечки, спровоцированной действиями вредоносной программы, которая распространялась посредством популярного приложения Cowboy Adventure. По предварительной информации, таким образом, были взломаны Facebook-аккаунты от 500 тыс. до 1 млн. пользователей.

3. Волна утечек данных накрыла компанию Facebook. Пострадали пользователи популярного приложения WhatsApp. Вредоносная программа TrojanSMS.Agent.ZS, ориентированная на программное обеспечение Android, маскируется под WhatsApp и распространяется через неофициальные магазины мобильных приложений. После загрузки поддельная программа предлагает пользователю внести плату за использование приложения. Затем TrojanSMS.Agent.ZS опустошает мобильный счет пользователя, совершая рассылку SMS на платные номера. Помимо этого, вредоносная программа самостоятельно совершает звонки и отправляет на удаленный сервер данные об устройстве и системе.

4. В начале 2014 года выяснилось, что все файлы, которыми обмениваются пользователи сервиса ICQ, принадлежащего Mail.ru Group, фактически находятся в открытом доступе. Виной тому – новая схема передачи файлов, введённая разработчиками после приобретения сервиса у AOL. Если раньше файлы передавались напрямую от пользователя к пользователю, то теперь файл сохранялся на сервере Mail.ru, а получателю отправлялась лишь ссылка для скачивания. При этом скачать файл по прямой ссылке мог кто угодно, никаких дополнительных проверок получателя не проводилось.

Финансовая оценка последствий инцидентов в сфере информационной безопасности является для специалистов вопросом актуальным и неоднозначным, так как даже скрупулёзное расследование и тщательная обработка инцидента не всегда дают полную картину. Особую сложность представляет оценка упущенной выгоды. Тем не менее, конкретные цифры убытка, пусть даже ориентировочные, необходимы в ежедневной работе для анализа рисков и обоснования использования тех или иных мер защиты информации.

Суммарные убытки компаний от утечек информации по разным оценкам составляют свыше $ 25 млрд. в год. В среднем организации теряют 31,23 млн. $ от каждой крупной утечки. В России убытки несколько меньше. При этом максимальные потери от одного инцидента составили около 4 млрд. руб.

Доля российских утечек в мировой статистике в 2015 году составила 6 %. Но она постоянно растет.

Большинство фиксируемых утечек (36,9 %) является следствием человеческих ошибок или халатности, но не злого умысла. Что, впрочем, не умаляет серьёзности последствий.

Борьба с угрозами данного вида может быть эффективной, если она основывается на следующих принципах:

– во-первых, соблюдение общих требований режима безопасности;

– во-вторых, создание собственной службы безопасности;

– в-третьих, обращение предпринимателей в соответствующие специализированные фирмы, агентства, оказывающие услуги по охране информации;

– в-четвертых, своевременное информирование правоохранительных органов.

Эффективная система защиты информации предусматривает несколько направлений деятельности по обеспечению безопасности бизнеса:

– защита информации о состоянии и движении материальных активов, чаще понимаемая как экономическая безопасность;

– защита информации о состоянии нематериальных активов и их носителях (персонале), определяемая как собственно информационная безопасность;

– защита средств хранения, обработки и передачи информации.

В разных странах существуют различные приоритетные направления защиты коммерческой информации (коммерческой тайны). Так, в Германии преобладают законодательные меры, в США и Франции, наряду с ними, предпочтение отдается организации собственных служб безопасности фирм, для Японии характерен корпоративный дух и долгосрочная занятость в фирме, а в Великобритании защита обеспечивается договорными обязательствами [2, с. 79].

Учитывая российскую специфику, выделяются следующие основные способы защиты информации, которые могут использоваться предпринимателями.

Законодательный. Основан на соблюдении прав предпринимателя на конфиденциальную информацию. При обнаружении нарушения прав предпринимателя как собственника, владельца или пользователя информации ему необходимо обратиться в соответствующие органы (МВД, ФСБ, прокуратуру, суд) для восстановления нарушенных прав и возмещения убытков.

Физическая защита – охрана, пропускной режим, специальные карточки для посторонних, закрывающиеся помещения, сейфы, шкаф и пр.

Организационный включает в себя:

– введение должности или службы, ответственной за отнесение определенной информации к категории конфиденциальной, соблюдение правил доступа и пользования этой информацией;

– разделение информации по степени конфиденциальности и организация допуска к конфиденциальной информации только в соответствии с должностью или с разрешения руководства;

– соблюдение правил пользования информацией (не выносить за пределы служебных помещений, не оставлять без присмотра во время обеда, включить сигнализацию при уходе);

– наличие постоянно действующей системы контроля за соблюдением правил доступа и пользования информацией (контроль может быть визуальный, документальный и др.).

Технический. Используются такие средства контроля и защиты как сигнализирующие устройства, видеокамеры, микрофоны, средства идентификации, а также программные средства защиты компьютерных систем от несанкционированного доступа.

Работа с кадрами. Предполагает активную работу кадровых служб фирмы по набору, проверке, обучению, расстановке, продвижению, стимулированию персонала. Следует регулярно проводить инструктажи персонала о необходимости соблюдения правил пользования конфиденциальной информацией и об ответственности за нарушения.

Часть этих способов предполагает значительные финансовые расходы, в связи, с чем использование всех способов одновременно по средствам только достаточно крупным и платежеспособным фирмам.

Изучение проблем защиты и сбора коммерческой информации свидетельствует о недостаточной правовой базе, регулирующий данный вопрос. При организации системы защиты информации в сфере предпринимательской деятельности необходимо, прежде всего, понимать, что при охране своего права на конфиденциальность, нельзя нарушать чужую, а также использовать незаконные средства сбора и охраны информации. Соблюдение этого принципа позволит сократить потери и не вступать в конфликт с законом.

Список литературы

1. Сердюк В. С. Возможные каналы утечки конфиденциальной информации через сеть Интернет // Журнал «Information Security. Информационная безопасность». – 2015. – № 6. – С. 27–30.

2. Шлыков В. В. Комплексное обеспечение экономической безопасности предприятия [Текст]. – СПб: «Алетейя». – 2014. – С. 78–82.

Газизова Д. Д.
Научный руководитель – преподаватель экономических дисциплин
Субботина Е. В.
Колледж Стерлитамакского филиала
ФГБОУ ВО «Башкирский государственный университет»
Республика Башкортостан, г. Стерлитамак

ЭКОНОМИЧЕСКИЙ ПОДХОД К ЗАЩИТЕ ИНФОРМАЦИИ

В условиях постоянно растущего потока информации возникает необходимость в разработке новых информационных технологий: обработки и хранения, развитие мощных компьютерных систем позволили повысить уровень защиты информации. Существующие сегодня средства, методы защиты информации, создают единый механизм экономической защиты, причем не только от злоумышленников, но и от некомпетентных или недостаточно подготовленных пользователей и персонала, а также нештатных ситуаций технического характера. Однако актуальной **проблемой** для коммерческих и государственных структур остается информационная система.

Главное направление поиска новых путей защиты информации заключается не просто в создании соответствующих механизмов, а в реализации роста процесса на всех этапах жизненного цикла систем обработки информации при комплексном использовании всех имеющихся средств защиты [1, с. 76].

К решению данной проблемы необходимо подходить комплексно. Одним из подходов является экономический подход. Он включает в себя:

1. Изучение вопросов экономической оценки информационных ресурсов.
2. Получение знаний о методах оценки угроз и степени риска в деятельности предприятия.
3. Знакомство с технико-экономическими задачами обеспечения информационной безопасности.
4. Формулирование и решение задач создания экономически обоснованных систем информационной безопасности (СИБ) предприятия.

Нетрудно увидеть, что цель защиты информации – надежность собственно информации, а не каналов связи, помещений и физических лиц. Исходя из этого, были определены технологии защиты данных, рекомендуемые для применения в коммерческом и государственном секторе.

Криптография или шифрование цифровой подписью.

В кодировании применяется пара ключей: открытый и закрытый, также цифровая подпись. Открытый и закрытый ключи в данном случае позволяют криптографическому алгоритму шифровать и кодировать информацию. При этом информацию, зашифрованную открытым ключом, расшифровать можно только с помощью закрытого ключа. Открытый ключ публикуется в сертификате владельца и доступен подключившемуся клиенту, а закрытый – хранится у владельца сертификата. Цифровая подпись заключается в использовании специальных способов проверки подписи.

Специальная программа проверки выясняет, является ли владелец ключа подписи автором данного документа.

Покупаем и экономим.

Стоимость системы защиты складывается из начальных вложений и стоимости эксплуатации, включающей в основном затраты на обучение персонала, поскольку расходы на поддержку продвигаемых на рынке систем практически нулевые.

Сегодня на рынке представлены программные продукты в трех ценовых категориях. Первая – до 1500 рублей за рабочее место, вторая – от 1500 до 6000 рублей за рабочее место, третья – свыше 6000 рублей за рабочее место. Системы защиты из первой категории разработаны неспециализированными компаниями, которые предлагают их в качестве приложения к основным продуктам. Для таких решений характерны низкий уровень проработки вопросов защиты информации, отсутствие возможностей доработки и обновления, а также плохая встраиваемость в бизнес-процесс и электронный документооборот.

В высшем ценовом диапазоне находятся программно-аппаратные комплексы, применение которых актуально в основном на государственных предприятиях. Однако есть продукты, которые продвигаются на коммерческий рынок при «попечительстве» отдельных ведомств.

Цена на основной класс продуктов, пользующихся наибольшим спросом, лежит в диапазоне 1500–6000 рублей. Оптимальным уровнем считается 3000–4000 рублей за рабочее место, включающее в себя реализацию всех трех технологий: кодирования, подписи и управления ключами.

Обслуживать такую систему может и один человек, хотя обычно этим занимаются два-три администратора. Таким образом, стоимость обслуживания может быть исчислена исходя из размера зарплаты и загруженности сотрудников, занимающихся ее эксплуатацией.

Внедряем и зарабатываем.

Внедрение системы защиты информации в корпоративную сеть позволяет наладить оборот электронных документов, конфиденциальной информации с обеспечением юридической значимости документов. Экономически это выгодно, поскольку: сокращается время прохождения документа; повышается надежность защиты коммерческой тайны.

Кроме того, существуют дополнительные положительные моменты, связанные с использованием защищенного документооборота: повышается персональная ответственность сотрудников; снижается риск от злонамеренных действий сотрудников; упрощается процедура работы с конфиденциальной информацией.

Виртуализация отношений поставщика услуг и клиентов диктует необходимость внедрять системы защиты информации в сети Интернет. Проведение финансовых операций с использованием Интернета, заказ товаров и услуг, использование кредитных карточек, доступ к закрытым информационным ресурсам, передача телефонных разговоров требуют обеспечения соответствующего уровня безопасности. Всегда существует проблема выбора между необходимым уровнем защиты и эффективностью работы в сети. В некоторых случаях пользователями или потребителями меры по обеспечению безопасности могут быть расценены как меры по ограничению доступа и эффективности. Однако такие средства, как, например, криптография, по-

зволяют значительно усилить степень защиты, не ограничивая доступ пользователей к данным. Затратная составляющая здесь может быть несколько выше, чем для корпоративной сети, но это себя оправдывает [3, с. 79].

Внедрение систем защиты информации в систему обслуживания клиентов приносит опосредованную прибыль, поскольку: сокращается время на обслуживание клиента, следовательно, появляется возможность принять большее количество клиентов за единицу времени; в связи с автоматизацией ряда процессов можно сократить персонал, занятый в обслуживании клиентов; скорость и удобство обслуживания привлекают новых клиентов.

Таким образом, защищаемая информация должна приносить определенную пользу ее собственнику и оправдывать затрачиваемые на ее защиту средства. Степень секретности обычно со временем уменьшается и реже увеличивается. Информация должна оставаться конфиденциальной до тех пор, пока этого требуют интересы государства или коммерческой деятельности предприятия. Для наиболее эффективного использования информации за время ее жизненного цикла, в течение которого она является актуальной, необходимо выбрать такой режим ее распространения, при котором эффект от использования информации с учетом позитивных и негативных последствий достигал бы максимальной величины. При таком подходе ограничение распространения информации на определенное время является одним из способов управления информационным ресурсом собственника в интересах достижения максимального эффекта от его использования.

Список литературы

1. Васильев И. В., Козин И. Д., Федулина И. Н. Защита информации. Учебное пособие. – Алматы: АУЭС, 2013. – 120 с.

2. Еженедельник «Директор-инфо» [Электронный ресурс] – URL: http://www.directorinfo.ru/article.aspx?id=13046&iid=511 (дата обращения 16.02.2017).

3. Цуканова О. А., Смирнов С. Б. Экономика защиты информации: Учебное пособие, 2-е издание, измененное и дополненное. – СПб.: НИУ ИТМО, 2014. – 240 с.

Гизатуллина Г. Р.
Научный руководитель – преподаватель математики и информатики
Лысенко Д. В.
Колледж Стерлитамакского филиала
ФГБОУ ВО «Башкирский государственный университет»
Республика Башкортостан, г. Стерлитамак

ВЛИЯНИЕ СЕТИ ИНТЕРНЕТ НА РАЗВИТИЕ ПОЗНАВАТЕЛЬНОЙ АКТИВНОСТИ МОЛОДЕЖИ

На современном историческом этапе жизнь людей, особенно молодёжи, тесно связана с использованием возможностей, предоставляемых глобальной сетью Интернет. Возникла новая информационная среда, в которой информация транслируется, укладывается и копируется практически мгновенно.

Данный фактор дал свои предпосылки для формирования новых реалий познавательной деятельности молодёжи.

Всё это делает актуальным научную работу по **проблеме** влияния сети Интернет на формирование познавательной активности молодежи.

Цель исследования данной научной работы состоит в изучении влияния сети Интернет на познавательную активность молодежи. Достижение поставленной цели предполагает решение следующих **задач**:

1. Установить степень приоритетности использования сети Интернет в процессе познавательной деятельности.

2. Сравнить уровень познавательной активности с использованием сети Интернет и без.

Гипотеза исследования заключается в предположении о том, что сеть Интернет оказывает значительное влияние на формирование познавательной активности молодежи.

Объектом исследования выступает молодежь от 16 до 19 лет, студенты колледжа СФ БашГУ.

Предметом исследования является влияние сети Интернет на формирование познавательной активности молодежи.

Познавательная активность – это интеллектуально-эмоциональная склонность к процессу познания. Познавательная активность направлена на приобретение определенного набора знаний, умений и навыков, необходимого для достижения личностью поставленных целей, и реализуется как в учебном процессе, так и в самостоятельной деятельности индивида. Источником познавательной активности является потребность в познании, самореализации, признании в обществе, материальном благополучии и др. [1].

Различают познавательную активность двух типов [2]:

- направленную на усвоение, приобретение, применение уже имеющегося в опыте индивида или человечества в целом (интеллектуальная деятельность, активность);

- создание совершенно нового, для чего в личном и общественном опыте еще не существует готовых образцов (творческая активность).

Для того чтобы определить уровень познавательной активности молодых людей, необходимо выяснить важность, самостоятельность и осознанность ими этого вида деятельности.

К объективным показателям степени познавательной активности молодежи относятся следующие:

- учебная успеваемость;
- временные затраты на познавательную деятельность;
- работа с Интернет-ресурсами образовательного направления, просмотр познавательных телепередач;
- уровень самостоятельности выполнения работ и т.д.

К субъективным показателям относятся:

- мотив обучения;
- уровень заинтересованности;
- оценка возможности использования полученных знаний и навыков;
- оценка степени влияния познавательной деятельности на достижение жизненных целей;
- планы относительно продолжения образования и т.д.

С учетом градаций возможных значений выбранных показателей, результаты определения уровня познавательной активности могут принять следующий вид:

- высокий уровень познавательной активности – знания и навыки их приобретения являются основной целью. Наиболее выраженной потребностью личности является потребность в познании. Высокий уровень всех объективных показателей;
- средний уровень познавательной активности познание – является средством достижения других целей, получение знаний не является первоочередной потребностью;
- низкий уровень познавательной активности – знание не является основной ценностью, осознается лишь необходимость его получения. Представления об использовании полученных знаний смутные;
- пассивность – отношение к познавательной деятельности негативное.

В России большое внимание на государственном уровне уделяется информатизации общества в целом и сферы образования, в частности. Реализуются федеральные, межведомственные и отраслевые программы, направленные на решение актуальных задач информатизации образования. В последнее время проведена огромная работа по сбору и систематизации образовательных ресурсов на федеральных образовательных порталах, основным из которых является портал «Российское образование» [3]. Так, в информационном пространстве, предоставляющем доступ к образовательным ресурсам можно выделить ряд направлений, стимулирующих развитие познавательной активности молодежи. Это федеральные и региональные образовательные ресурсы, конференции, выставки, конкурсы, олимпиады, инструментальные программные средства, энциклопедии, словари, справочники, образовательная пресса, ресурсы дистанционных форм обучения.

В настоящее время продолжается интенсивный рост числа сайтов, содержащих образовательные ресурсы. Характерной особенностью Интернет-ресурсов является

то, что каждый из них имеет свою аудиторию, т.е. фактически организовывается сетевое сообщество из заинтересованных посетителей.

На основе проведенного нами исследования (анкетный опрос студентов колледжа СФ БашГУ) стало возможным провести социологический анализ социальной активности молодежи и попытаться понять, в какой степени ресурсы сети Интернет могут стать ресурсом формирования познавательной активности.

Результаты исследования показали, что молодежь почти вся (100 %) включена в использование сети Интернет. Основной целью использования Интернета молодежью являются:

- «обучение» – 30,4 %;
- «общение» – 26,1 %;
- «развлечение» – 21,7 %;
- «поиск справочных материалов, просмотр новостей» – 21,7 %.

Таким образом, практически повсеместная доступность сети Интернет привела к тому, что молодые люди практически все свое свободное, да и не только свободное, проводят в сети Интернет: общаются, ищут информацию, организуют досуг.

Для того чтобы сравнить уровень познавательной активности с использованием сети Интернет и без, опрошенным был задан вопрос: Вы по желанию согласились взяться за написание реферата, но вскоре узнали, что обязательным условием является запрет на пользование Интернет-ресурсами. Отказались бы Вы от задуманного? 86,9 % опрошенных отказались от написания. Как показывает данный эксперимент, Интернет играет значительную роль в формировании познавательной активности молодежи, её уровень повышается благодаря использованию глобальной сети. Гипотеза доказана, сеть Интернет значительно влияет на формирование познавательной активности молодежи.

Проведенные исследования позволяют прийти к следующим выводам. Одной из основных целей использования сети Интернет молодежью является работа с Интернет-ресурсами образовательного направления. Использование Интернет технологий значительно расширяет возможности представления информации, что позволяет усилить познавательную активность молодежи. Поиск информации с использованием современных технических средств и новых информационных технологий тренирует и активизирует память, наблюдательность, сообразительность, концентрирует внимание, заставляет оценивать предлагаемую информацию. Именно в информационном пространстве, предоставляющем доступ к образовательным ресурсам, развиваются новые направления, стимулирующие развитие познавательной активности молодежи.

Список литературы

1. Джерри Д., Джерри Дж. Большой толковый социологический словарь: основные термины и понятия по социологии. В 2 т.: Т. 2: П-Я (пер. с англ. Марчук Н. Н.). Изд-во: Вече. АСТ, Т. 2. – 2001. – С. 67.

2. Левитес Д. Г. Практика обучения: современные образовательные технологии. – Воронеж, 1998. – 226 с.

3. Российское образование. Федеральный образовательный портал: учреждения, программы, стандарты, вузы, тесты ЕГЭ. URL: http://www.edu.ru

Даянова Р. Р.
Научный руководитель – преподаватель юридических дисциплин
Романова А. П.
Колледж Стерлитамакского филиала
ФГБОУ ВО «Башкирский государственный университет»
Республика Башкортостан, г. Стерлитамак

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В СФЕРЕ СОЦИАЛЬНОГО ОБЕСПЕЧЕНИЯ

Информация – важнейший продукт общественного производства, постоянно наращиваемый ресурс человечества. Сегодня это наиболее ценный и ходовой объект в международных экономических и социальных отношениях.

Вся информация представляет различную ценность и, соответственно, ее разглашение может привести к угрозам безопасности различной степени тяжести. Боязнь лишиться таких активов заставляет создавать различные системы защиты, в том числе и организационную, а главное – правовую.

В современном обществе неизбежность и целесообразность использования информационных технологий и глобальных коммуникаций влечет за собой неотвратимость угроз информационной безопасности и утечке «закрытой» информации.

Проблема защиты персональной (конфиденциальной) информации органов муниципального самоуправления в настоящее время стоит наиболее остро, так как угрозы нарушения информационной безопасности носят глобальный и трансграничный характер; способы реализации угроз информационной безопасности и формы их проявления постоянно совершенствуются; высокая технологичность этих угроз требует адекватных мер противодействия, предъявляет требования к квалификации специалистов по информационной безопасности.

Термин «информация» происходит от латинского слова «informatio», что означает сведения, разъяснения, изложение. Несмотря на широкое распространение этого термина, понятие информации является одним из самых дискуссионных в науке. В настоящее время наука пытается найти общие свойства и закономерности, присущие многогранному понятию информация, но пока это понятие во многом остается интуитивным и получает различные смысловые наполнения в различных отраслях человеческой деятельности.

Информация играет огромную, ведущую роль в жизнедеятельности каждого предприятия и организации. Для любого субъекта информационных отношений наиболее важны и ценны те сведения, которыми владеют или пользуются только они и никто больше.

Учитывая особенную и, пожалуй, вечную актуальность темы поиска и сохранения информации, государство должно установить для всех «правила игры» на этом поле, гарантировав субъектам информационных отношений права и установив определенные обязанности, специальные ограничения и санкции, то есть полностью в правовом смысле отрегулировать всю систему оборота информации, особенно той,

на которую субъекты права имеют или хотят иметь преимущества в использовании, – конфиденциальной.

Защита персональных данных – это комплекс мероприятий, позволяющий выполнить требования законодательства РФ, касающиеся обработки, хранения и передачи персональных данных граждан.

Согласно требованию закона о защите персональных данных, оператор персональных данных обязан выполнить ряд организационных и технических мер касающихся процессов обработки персональных данных.

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Оператор персональных данных – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

К нормативно-правовым актам по защите персональных данных относят: Конвенцию о защите физических лиц при автоматизированной обработке персональных данных, Конституцию Российской Федерации, Основы законодательства Российской Федерации об охране здоровья граждан, Распоряжение Правительства Российской Федерации от 15 августа 2007 г. № 1055-р «Об утверждении Плана подготовки проектов нормативных правовых актов, необходимых для реализации Федерального закона «О персональных данных» и многие другие.

Положение с персональными данными в России (в том числе, с рынком персональных данных), мягко говоря, можно назвать удручающим.

В Российской Федерации, кроме конституционных положений, гарантирующих защиту частных интересов, в том числе персональных данных граждан, существуют только общие нормы [2, 3, 5, 6]. Фактически, это привело к положению, которое можно охарактеризовать как хаос.

В первую очередь, отсутствие норм, регламентирующих сбор, обработку и раскрытие персональных данных государственными структурами всех уровней, ведет de facto к безнаказанности лиц, делающих государственные базы персональных данных источником преступного извлечения прибыли. Ниже перечислено только ничтожно малое число подобных баз данных, открыто предлагаемых покупателям:

- «ЕГТС 20.0». Информация по владельцам телефонов (в т.ч. сотовых телефонов) – частным лицам с указанием ФИО и даты рождения по Московскому региону. Данные на октябрь 2002 года;
- «Собственники Московских Квартир» – информация о владельцах квартир в г. Москве, с указанием паспортных данных, даты приватизации (покупки), других совладельцев и т.д.;
- «Жилой Фонд Москвы». База Московского Департамента Муниципального Жилья и многие другие [1, с. 65].

К каким последствиям может привести бесконтрольное использование этой информации, можно только догадываться.

Во-вторых, законопослушные граждане лишены возможности на законных основаниях получить от государства необходимую им персональную информацию в том объеме и в той форме, которые не нарушают законных интересов субъектов данных. Граждане лишены также возможности влиять на точность и достоверность персональной информации, находящейся у государства, что явным и существенным образом влияет на защиту их прав.

Наконец, отсутствие норм, регулирующих оборот персональных данных на рынке, приводит не только к ущемлению прав граждан, чьи персональные данные стали объектом купли/продажи, но и тормозит создание цивилизованной системы услуг по предоставлению персональной информации.

Все эти проблемы должны быть решены в специальном законе о персональных данных. Актуальность этого закона подчеркивается также подписанием Россией в 2001 году европейской «Конвенции о защите физических лиц при автоматизированной обработке персональных данных», в которой сказано о необходимости каждой подписавшей стороне принять необходимые меры по реализации принципов защиты персональных данных в своем национальном праве.

Исполнить требования закона о персональных данных будет не столь уж трудно, если данную работу начать сейчас, не дожидаясь поступления первых заявлений и жалоб. Начать можно со следующих очевидных мер.

Желательно назначить ответственного сотрудника для рассмотрения всех вопросов, связанных с исполнением данного закона в организации, а для крупных компаний может быть оправдано создание специальной комиссии [4, с. 132].

Для всех информационных ресурсов организации, содержащих персональные данные, необходимо: определить их статус (на основании чего созданы: в соответствии с законодательством, для исполнения договора, по собственной инициативе и т.д.); уточнить и зафиксировать состав персональных данных и их источники получения (от гражданина, из публичных источников, от третьих лиц и т.д.); установить сроки хранения и сроки обработки данных в каждом информационном ресурсе; определить способы обработки; определить лиц, имеющих доступ к данным; сформулировать юридические последствия; определить порядок реагирования на обращения, возможные варианты ответов и действий, оценить реальность соблюдения установленных законом сроков реагирования.

Таким образом, несмотря на проводимые в современном государстве мероприятия в сфере защиты персональной (конфиденциальной) информации, все еще остается немало неразрешенных проблем, требующих оперативного вмешательства. Актуализация мер по сохранности данной информации, привлечение высококвалифицированных сотрудников, ужесточение наказаний за несанкционированный доступ к такой информации любых посторонних лиц, помогут не только устранить выявленные проблемы, но и усовершенствовать действующую систему защиты персональных данных.

Список литературы

1. Внуков А. А. Защита информации. – 2-е изд., испр. и доп. – М.: Изд-во «Юрайт», 2017. – 261 с.

2. Всеобщая декларация прав человека (принята Генеральной Ассамблеей ООН 10.12.1948) // Российская газета. – 10.12.1998.

3. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 г.). – М.: Норма, 2002. – 128 с.

4. Нестеров С. А. Информационная безопасность: учебник и практикум. – М.: Изд-во «Юрайт», 2017. – 321 с.

5. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (ред. 03.07.2016) // Российская газета. – 29.07.2006 – № 4131.

6. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. 19.12.2016) // Российская газета. – 29.07.2006 – № 4131.

Егорова Д. Д.
Научный руководитель – учитель истории и обществознания
Строчко Т. Н.
МБОУ «СОШ № 24 с углубленным изучением иностранного языка»
Республика Башкортостан, г. Салават

ВИРТУАЛЬНОЕ ПРОСТРАНСТВО СЕТИ ИНТЕРНЕТ – СОВРЕМЕННЫЙ АГЕНТ СОЦИАЛИЗАЦИИ

В течение последних десятилетий наблюдается интенсивное развитие информационных технологий, а также увеличение числа пользователей Интернета среди детей дошкольного и школьного возраста. Всемирная глобальная сеть – это, в первую очередь, источник информации, которая может стать не только благом, но и большой опасностью. В современном мировом сообществе постоянно происходят преобразования в социально-культурной и экономической сфере, что весьма интенсивно воздействует на различные стороны жизнедеятельности личности. Перед обществом в связи с этим появляются новые проблемы социализации подрастающего поколения. Эта тема очень **актуальна** в наш век цифровых технологий, так как интенсивная информатизация всех сфер дает как положительные плоды, так и отрицательные. Мы бы хотели рассмотреть **проблему** негативного влияния Интернета на подрастающее поколение.

Цель работы: выявить и обосновать роль Интернета на социализацию личности.

Задачи:

- определить идеологическое направление, присущее динамично развивающемуся Интернету;
- выявить роль идеологии в социализации личности;
- рассмотреть возможные практические решения проблемы доступного Интернета.

Под социализацией мы понимаем процесс интеграции человека в общество (в ту или иную группу) и в то же время обособление индивидуума.

К основным агентам социализации относятся: семья, школа, сверстники, СМИ и Интернет.

Клаус Шнеевинд понимает под семьей некую совокупность индивидов, удовлетворяющую четырём критериям [3]: 1) психическая, духовная и эмоциональная бли-

зость её членов; 2) пространственная и временная ограниченность; 3) закрытость, межличностная интимность; 4) длительность отношений, ответственность друг за друга, обязанность друг перед другом.

Многие дети еще в дошкольном возрасте становятся активными пользователями Интернета. Кому-то предоставляется полная свобода, когда родители ни в коей мере не ограничивают своего ребёнка в часах, проводимых за компьютером и в Интернете. Кто-то сам предоставляет себе эту свободу, в то время как родителям просто не удается уследить за своим чадом. Тем не менее, в таких ситуациях ближайшее окружение в лице родителей в полной мере ответственны за те последствия, положительные или отрицательные, которые за собой повлечет активное приобщение к Интернету детей-дошкольников.

В современном формирующемся в России информационном обществе институты социализации семья и образование, постепенно уступают свои позиции другим агентам социализации – средствам массовой информации и Интернету.

Масштабы компьютеризации и интернетизации общества настолько велики, что они не обходят стороной и современное образование. Если ребёнок в ранние годы своей жизни был изолирован, частично или полностью, от компьютера, и Интернета в частности, то обучение в школе полностью восполняет эти пробелы. Создание компьютерных классов, использование Интернета на уроках, школьные творческие задания, которые требуют от ученика наличия навыков работы на компьютере и в Интернете – всё это является одной из объективных причин освоения подростком «нового жизненного пространства» – киберпространства.

Поэтому очень важно обучать школьников позитивному использованию возможностей и ресурсов Интернета как социокультурного феномена и современного социального института, учитывать мощный социализирующий и воспитательный потенциал Интернет-среды. В противном случае, школьники могут испытывать на себе негативные последствия киберсоциализации: например, воспринимать виртуальное пространство как реальный мир, способ уйти от действительности, или, наоборот, испытывать неоправданный страх перед передовыми технологиями, вплоть до технофобии [1].

Помимо этого сегодня существует проблема распространения и навязывания посредством Интернета информации, которая не отвечает общечеловеческим этическим и эстетичным идеалам и нормам морали. Как результат, виртуальное пространство и доступность информации там становится для школьника, как огромной возможностью, так и настоящей катастрофой. Поэтому актуальным является вопрос о том, как обезопасить ребёнка в процессе его социализации от негативного влияния Интернет-среды. Этого можно добиться путем осуществления просветительской деятельности по ознакомлению детей с Интернетом как феноменом современного мира, с существующими возможностями Интернет-пространства, а также потенциальными опасностями. Это позволит детям лучше ориентироваться в виртуальном мире и корректировать свой опыт киберсоциализации. Подобная просветительская работа должна исходить, в первую очередь, от государства, которое способно финансировать программы тренингов, как для детей, так и для их родителей, способствовать созданию условий для повышения квалификации учителей благодаря специально

организованным методическим собраниям по проблемам киберсоциализации школьников в Интернет-пространстве.

На рубеже XX–XXI вв. появляется социально-педагогический феномен – киберсоциализация человека. Термин «виртуальная компьютерная социализация» вошел в употребление в научных кругах благодаря В. А. Плешакову [2, с. 208]. На наш взгляд данная проблема является глобальной. Она охватила весь мир, подключенный к сети Интернет.

Школьники как пользователи сети Интернет находят удовлетворение собственных актуальных потребностей личности, которые можно описать с помощью пирамиды А. Маслоу.

Главным фактором Интернета как агента социализации является принцип свободы, не только слова, но и действия. Интернет как агент социализации молодежи оказывает сильнейшее воздействие на личность и ее нравственное состояние: виртуальный мир, в который попадает молодой человек, дает ему дополнительную свободу для выражения своих эмоций, чувств, жизненных позиций, настроений, взглядов, преодоления различного рода внутренних и внешних конфликтов, возникающих в реальной жизни в семейных отношениях, отношениях со сверстниками. Интернет, усиливая процесс опосредованного общения, оказывает воздействие на психическое состояние личности в плане формирования Интернет-зависимости. Еще одно изменение 21 века – создание социальных сетей. Социальные сети – это структура, которая базируется на человеческих связях или взаимных интересах. В качестве Интернет-сервиса социальная сеть может рассматриваться как платформа, с помощью которой люди могут осуществлять связь между собой и объединяться по специфическим интересам. Задача такого сайта заключается в том, чтобы обеспечить пользователей всеми возможными путями для взаимодействия друг с другом – видео, чаты, изображения, музыка, блоги и другое.

Особого внимания заслуживает такая проблема влияния на социализацию личности, как распространение в глобальных сетях игр с элементами насилия. В частности, известны случаи, когда подростки под влиянием данных жестоких сетевых игр расстреливали своих одноклассников.

Исходя из всего вышесказанного, мы приходим к выводу, что функционирующая в глобальных сетях среда способна оказывать существенное влияние на формирование негативных психологических и поведенческих установок подростков, что актуализирует обращение к базовым агентам социализации, в первую очередь семье.

Для того чтобы максимизировать эффект позитивной социализации старших школьников посредством Интернета, необходимо сообща, путем интеграции усилий институтов семьи и среднего образования, создать такие условия, при которых Интернет стал бы одним из эффективных агентов социализации современной молодёжи. Это может быть постоянный мониторинг и повышение социального и воспитательно-образовательного потенциала Интернет-среды, активное использование Интернета в воспитательно-образовательных целях, реализуемых как школой, так и членами семьи, привлечение должного внимания к проблемам социализации старших школьников в Интернете со стороны государства и общества.

В рамках традиционных социальных институтов социализация осуществлялась в процессе коммуникации личности с окружением. При этом количество персонифи-

цированных агентов социализации было относительно невелико в силу чисто физических (время и место) ограничений возможности контактировать с представителями социума. Иными словами, человек в одно и то же время и в одном и том же месте может общаться с относительно малым количеством людей. Принципиально иным образом дело обстоит в ситуации Интернет-коммуникации. Здесь в режиме реального времени личность может вступать в практически неограниченное количество коммуникаций за счет использования таких технологий как чаты, блоги и пр. Здесь нет необходимости перемещаться в пространстве для поиска партнеров по общению, что позволяет иметь контакты с людьми, находящимися практически в любых уголках планеты. В Интернете возникает возможность менять пол, возраст, социальный статус и тем самым «примерять» на себя различные социальные роли, не подвергаясь риску потерпеть неудачу. В целом в Интернет-среде возникают невиданные прежде возможности создания виртуальной личности и экспериментирование с идентичностью. Как представляется, мы находимся на том этапе, когда есть возможность не только изучать влияние Интернета на социализацию, но и прогнозировать и пытаться наметить пути управления этим процессом. Меры могут быть разные, от законодательного ограничения некоторых аспектов пользования Интернет до формирования позитивных жизненных установок и шире – культуры пользования Интернет.

Список литературы

1. Плешаков В. А., Угольков Н. В. Интернет как фактор социализации старших школьников // Философские проблемы информационных технологий и киберпространства. – 2012. – № 1. – С. 16–22.

2. Плешаков В. А., Леванова Е. А., Волошина А. Г., Соболева А. Н., Телегина И. О. Игра в тренинге. Возможности игрового взаимодействия. – 3-е изд. – СПб.: Питер, 2013. – 208 с.

3. Семья // Википедия. [2017–2017]. Дата обновления: 30.01.2017. URL: http://ru.wikipedia.org/?oldid=83809390 (дата обращения: 30.01.2017).

Еронова Д. А.
Научный руководитель – преподаватель математики и информатики
Артемьев А. В.
Колледж Стерлитамакского филиала
ФГБОУ ВО «Башкирский государственный университет»
Республика Башкортостан, г. Стерлитамак

РЕАЛЬНАЯ И ВИРТУАЛЬНАЯ ЖИЗНЬ СОВРЕМЕННОЙ МОЛОДЕЖИ

Всемирная сеть стала неотъемлемой частью жизни любого человека: с ее помощью осуществляются работа, учеба, отдых, развлечения, оказываются услуги, совершаются покупки. Необъятное виртуальное пространство привлекает все больше и больше людей, которые стремятся найти здесь информацию, удовлетворить потребности в общении, шопинге, развлечениях. Самыми активными пользователями сети Интернет на сегодняшний день являются молодые люди и девушки, для которых наиболее привлекательными оказались всевозможные социальные сети, онлайн-дневники, чаты, компьютерные игры, поисковые системы. Интернет обладает массой достоинств, которые облегчают повседневную жизнь современного человека. Благодаря научно-техническому прогрессу ежедневное общение и обмен информацией стали происходить быстрее и удобнее.

Интернет делают притягательным следующие свойства [3]: 1) возможность анонимного общения, т.е. люди, могут общаться друг с другом без имени, пользуясь условным «логином», присвоенным при регистрации; 2) возможность интерактивной реализации представлений, фантазий, невозможных в обычном мире (в том числе создание новых образов «Я» в ролевых играх, чатах и т. д.); 3) возможность поиска нового собеседника, удовлетворяющего практически любым качествам (заметим, что нет необходимости удерживать внимание одного собеседника – в любой момент можно найти нового).

Несмотря на безусловную пользу и удобство Интернета, недостатки здесь тоже имеются и немалые. Попадая в виртуальный мир, молодежь лихорадочно «блуждает» по сети, зачастую забывая о ежедневных делах, учебе и работе, о взятых на себя обязательствах, полностью «растворяясь» в манящих и красочных сайтах. В подобных случаях речь идет об Интернет-зависимости или так называемой Интернет-аддикции. Интернет-аддикция – это непреодолимое желание подключиться к Интернету в режиме офлайн и неспособность завершить сеанс, находясь в режиме онлайн [2]. Многие люди, находясь в социальных сетях, не замечают, как быстро течет время и насколько они привязаны к потоку информации, поступающей ежеминутно, насколько трудно выключить компьютер и обратить внимание на реальные предметы.

По мнению психолога М. И. Дрепы [1], существуют несколько видов зависимости от Всемирной паутины: 1) навязчивый веб-серфинг (информационная перегрузка) – бесконечные путешествия по Всемирной паутине, поиск информации; 2) пристрастие к виртуальному общению и виртуальным знакомствам – большие объёмы переписки, постоянное участие в чатах, веб-форумах, избыток знакомых и друзей в сети; 3) игровая зависимость – навязчивое увлечение компьютерными играми по се-

ти; 4) навязчивая финансовая потребность – игра по сети в азартные игры, ненужные покупки в Интернет-магазинах или постоянные участия в Интернет-аукционах.

При такой зависимости человек перестает искать свою реальную жизненную дорогу, откладывая в «долгий ящик» дела, затормаживая тем самым социальное и личностное развитие. На физиологическом уровне появляется вялость, сонливость, раздражительность, тревожность, проявляется снижение работоспособности, ухудшение памяти и внимания. Свободный доступ в Интернет отбивает желание развивать взаимодействие и строить отношения с обществом на реальном, не виртуальном уровне. Это особенно заметно среди подростков и молодых людей юношеского возраста.

Последствиями продолжительного онлайн-существования становятся проблемы в обучении, снижение умственной активности, частые и беспричинные смены настроения, неадекватная реакция на критику, эмоциональное отчуждение, нарастающая оппозиционность и негативное отношение к окружающим, требующим выключить компьютер, отказ от других интересов и хобби, приступы страха, агрессии, тревоги, появление фобий, изворотливость, лживость, замкнутость, ранее не характерные личности.

В связи с поставленными выше проблемами в феврале 2017 года на базе Стерлитамакского филиала Башкирского государственного университета организовано прикладное эмпирическое исследование влияние виртуального пространства сети Интернет на жизненные ценности современной молодежи, в котором приняли участие студенты колледжа в возрасте от 15 до 20 лет. Для респондентов (всего участвовало 60 человек) была разработана анонимная анкета. В ходе анализа результатов анкетирования было выявлено, что все студенты, участвовавшие в анкетировании (100 %), каждую свободную секунду посвящают общению в сети, поиску информации или онлайн-играм. На первый вопрос анкеты «Сколько времени вы проводите в Интернете?» 70 % опрашиваемых ответили, что уделяют этому более трех часов в день и только 30 % опрашиваемых осознают, что уделяют слишком много времени веб-серфингу, бесполезно теряя драгоценное время, что является психологической зависимостью от виртуального пространства. Следовательно, Интернет (как социальные сети и информационный источник) становится неотъемлемой частью жизни и жизненной ценностью для молодежи. В ходе анализа ответов респондентов установлено, что в социальных сетях ежедневно проводят огромное количество времени 60 % опрашиваемых, в основном для обмена информацией на вербальном и мультимедийном уровнях, что удобно и дает возможность общаться на значительном расстоянии друг от друга, не выходя из дома. Однако 15 % отвечающих подчеркнули, что живое общение, стало отходить на второй план, в некоторых случаях Интернет заменяет им реальность, что зачастую, выйдя для виртуального общения в социальные сети, они отказываются от прогулок, встреч, непосредственного взаимодействия с близкими. Треть респондентов заметили, что стали реже видеться с друзьями, отдавая предпочтение переписке в чатах и социальных сетях. Основная опасность глобальной сети Интернет в иллюзорности воспринимаемой и получаемой информации – личность на самом деле находится в одиночестве перед электронным устройством, а у нее создается иллюзия полноценного общения. Сидя перед экраном монитора, молодой человек получает колоссальный объем информации, который не в состоянии предоставить внешний мир в отличие от виртуального. Оставшаяся часть опрошенных студентов (85 %) считает, что Интернет слабо влияет на общение в «реале», подчеркивает плюсы социальных сетей и форумов – это новые знакомства, ко-

торые могут перерасти в более близкие отношения, поиск единомышленников, общение с одногруппниками или родственниками, которые проживают в другом городе или чужой стране. В ходе анкетирования мы получили информацию о том, какие сайты являются самыми популярными для современного молодого человека. По результатам анкетирования 20 % обучающихся постоянно обращаются к поисковым Интернет-ресурсам, электронным библиотекам и архивам. Чтобы расслабиться и отдохнуть – 15 % респондентов используют игровые сайты. Опрашиваемые студенты признались, что игры в сети Интернет стали потребностью, что часто они не способны своевременно завершить сеанс, возникает непреодолимая тяга изучить все уровни и стратегии, предлагаемые разработчиком игры. Большинство респондентов согласны, что существуют иные способы развлечения и отдыха, но популярность Интернета состоит именно в доступности, мобильности, простоте и удобстве использования, его интерактивности. Стоит отметить, что сайты знакомств не пользуются популярностью у современной молодежи студенческого возраста (0 % опрошенных). Молодые люди негативно относятся к знакомствам через социальные сети и имеют традиционные представления о том, как и где лучше заводить знакомства: в неформальной обстановке интересного общественного места (кафе, парк, кинотеатр и пр.). «Интернет является полезным открытием и познавательной средой для любого вида деятельности» – так заявили 51 % опрошенных студентов. Действительно, стоит выйти в информационно-поисковую систему, и вы получаете доступ ко всем областям знаний – от библиотеки Конгресса США до заметки в газете «Комсомольская правда». Треть молодых людей (33 %) высказалась за то, что длительное нахождение в сети – пустая трата времени. Данные респонденты утверждают важность таких жизненных ценностей, как привязанность и любовь, приятное времяпрепровождение, удовольствия, отдых, общение, признание и уважение других людей, высокое материальное благосостояние.

Анализ данных результатов анкетирования выявил следующие фактические данные: половина опрошенных честно признались, что онлайн-общение стало частью жизни, и отмечают тенденцию к замене живого общения виртуальным, а 18 % опрошенных не представляют своего существования без Интернета. У 60 % юношей и девушек возникает ежедневная потребность в использовании Интернета, связанная с учебой или работой, с поиском информации, проблема лишь в ее корректности и достоверности. 44 % – периодически пользуются просторами всемирной паутины, 16 % опрошенных признались, что развлекательные и коммуникативные ресурсы сети отвлекают от важных дел. Порадовало то, что 40 % студентов утверждают, что предпочитают активную, творческую и познавательную деятельность стационарному пребыванию перед монитором. Таким образом, Интернет оказывает значительное влияние на ценностные ориентиры молодежи, он плотно вошел в обиход современного человека, грань между виртуальностью и реальностью стала очень тонкой. Недостаточно социализированные и слабые характером личности попадают под «волны» веб-пространства, полностью погружаясь в разнообразные сайты, социальные сети, чаты, форумы, онлайн-игры.

Постепенно обесценивается живое полноценное общение, реальный коммуникативный акт с его непосредственными эмоциями заменяется бесчувственными сухими сообщениями, чтение книг – сомнительной информацией поисковых сайтов, психологическое здоровье – зависимостью от IT-технологий и виртуального информационного пространства.

Список литературы

1. Дрепа М. И. Интернет-зависимость как объект научной рефлексии в современной психологии // Знание. Понимание. Умение. – 2009. – № 2. – С. 189–193.

2. Кузнецова Л. Э., Ерошенко А. Н. Психологические особенности проявления виктимного поведения у современной молодежи [Текст] // Актуальные вопросы современной психологии: материалы II Междунар. науч. конф. (г. Челябинск, февраль 2013 г.). – Челябинск: Два комсомольца, 2013. – С. 73–75.

3. Патрикеева Э. Г., Соловьева О. А., Селезнева Т. А. Влияние виртуального пространства сети Интернет на жизненные ценности современной молодежи // Молодой ученый. – 2015. – № 10. – С. 1342–1346.

Заводчиков Д. Е.
Научный руководитель – учитель истории и обществознания
Аблеева Н. В.
МБОУ «СОШ № 24 с углубленным изучением иностранного языка»
Республика Башкортостан, г. Салават

СПОСОБЫ ПРОТИВОСТОЯНИЯ ХАКЕРСКИМ АТАКАМ И ЭФФЕКТИВНОЙ ЗАЩИТЕ ИНФОРМАЦИИ

На наш взгляд, тема защиты персональных данных в настоящее время особенно **актуальна**, т. к. увеличивающийся объем массивов информации вызывает появление новых правовых проблем, требующих принятия адекватных мер реагирования.

Цель работы – ознакомление со способами противостояния хакерским атакам и способами защиты информации.

Задачи, осуществление которых важно для надёжной защиты информации:

1. Создание внутренней документации по работе с персональными данными;
2. Организацию системы защиты персональных данных;
3. Внедрение технических мер защиты персональных данных.

Проблема информационной безопасности превращается в последнее время из гипотетической во вполне реальную. Количество угроз растет с каждым днем, изменяется нормативно-правовая база, соответственно реалиям времени должны изменяться и методы обеспечения информационной безопасности.

«Кто владеет информацией, тот правит миром» – эти слова Н. Ротшильда приобретают все более весомое значение в наше время. В данной статье мы хотим описать собственное видение проблемы и пути ее решения.

В проблеме обеспечения информационной безопасности четко выделяются технический, организационный и документационный аспекты. Технический аспект связан с выбором программного обеспечения, организационный – с проведением мероприятий для реализации закона № 152-ФЗ «О персональных данных»[4, с. 4], а документационный – с созданием локальных актов. Однако в современном информационном обществе организационный и документационный аспекты в значительной мере перекрываются.

В первую очередь рассмотрим технические вопросы. Для студентов главным способом поиска информации является использование глобальной сети Интернет. Какие угрозы существуют в Интернете? Это компьютерное мошенничество, компьютерные вирусы, хакерские атаки, вандализм, хищение, разглашение конфиденциальной информации и так далее. Противостоять им можно с помощью программы, осуществляющей фильтрацию входящего трафика (прокси-сервера). Например, такой программой может стать UserGate. Это удачное комплексное решение для организации общего доступа в Интернет из локальной сети, учета трафика и защиты от внешних угроз, а сетевой экран надежно защищает сеть от внешних атак. По необходимости можно подключать к Интернету даже компьютерные классы или отключать их, задавать временные отрезки для работы в Интернете, блокировать нежелательные ресурсы по отдельности, либо по категориям сайтов. Использование прокси-сервера также позволит контролировать и объем скачиваемых из сети данных, что значительно уменьшит нагрузку на локальную сеть. Кроме того, использование грамотно настроенной антивирусной программы, с автоматическим обновлением и сформированным дополнительным списком угроз (в случае нашего колледжа – Касперский 6.0) дает, в свою очередь, качественную антивирусную защиту.

Бич сегодняшнего времени – вирусы «автораны», переносимые флэш-накопителями, блокируются у нас при помощи отключения возможности автозапуска на любых носителях, а также специальным образом организованной структурой хранения данных на флэш-накопителе. Для этого проводятся краткие обучающие занятия по защите информации для сотрудников, студентов, рабочих информационной индустрии.

Еще один канал распространения угроз – электронная почта, которой пользуются практически все. Самый надежный способ контроля – организация собственного почтового сервера, с помощью которого проще отслеживать почтовые протоколы, фильтровать нежелательные или сомнительные «послания». В этом случае у всех сотрудников есть свой почтовый адрес на собственном почтовом сервере компании и запрещён служебный документооборот через сторонние сервера. Однако это идеальный вариант, и осуществлен он будет в недалеком будущем, пока же просто усилен контроль за ресурсами, посещаемыми сотрудниками.

Еще одной технической стороной проблемы бесперебойной работы компьютеров является разграничение доступа к информации и к ресурсам компьютера. Наличие как минимум двух учетных записей (одна с ограниченными правами – основная, а вторая с правами администратора – только для настроек и обе обязательно под паролем) позволяет намного дольше сохранить работоспособность компьютерного парка в целом, контролировать установку программного обеспечения. Таким образом, установка контрафактного и «зловредного» ПО, в большинстве случаев, просто невозможна (не достаточно полномочий).

Второй аспект проблемы информационной безопасности – организационный. Это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба. Для успешной работы все участники должны четко осознавать проблему информационной безопасности. Пока же пользователи нередко нарушают порядок обработки информации, не соблюдают требования нормативно-правовых до-

кументов, регламентирующих информационную безопасность. Безопасность информации может быть обеспечена только при комплексном использовании всех средств защиты. Процесс построения системы информационной безопасности не может быть разовым мероприятием, равно как исполнение и контроль не может быть возложен на одного ответственного за информационную безопасность. Этот процесс должен быть управляемым, постоянно совершенствуемым. Такой подход – стратегическое звено во всей системе информационной безопасности, также как информация – главный защищаемый элемент.

Положения о защите персональных данных работников регламентируются:

- Конституцией Российской Федерации.
- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».
- Трудовым кодексом РФ.

Во исполнение Закона № 152-ФЗ в первую очередь, было проведено внутреннее обследование информационной системы колледжа и определен ее класс – К3, в соответствии с этим разработаны: уведомление для Роскомнадзора, приказ об ответственных лицах по сотрудникам, а также положение о защите персональных данных. Такое положение является основным локальным актом и было принято с учетом мнения первичной профсоюзной организации учреждения в порядке, предусмотренном ст. 372 Трудового Кодекса РФ [6, с. 4].

Этот документ определяет: порядок обработки персональных данных работников; обеспечение защиты прав и свобод работников при обработке их персональных данных; ответственность лиц, имеющих доступ к персональным данным работников, за невыполнение правовых норм, регулирующих обработку и защиту персональных данных работников.

Далее, исходя из рекомендаций, данных в Законе, была создана рабочая группа, в которую вошли юрист, специалист по кадровой работе и специалист по информационным технологиям. Поскольку главным условием защиты персональных данных является четкая регламентация функций сотрудников, то рабочей группой были проведены также следующие мероприятия: уточнены все ситуации, когда требуется проводить обработку персональных данных, четко выделены процессы, в которых обрабатываются персональные данные, начата разработка пакета организационно-распорядительных документов для обеспечения полноценной защиты.

Не стоит забывать, что специфика информационных учреждений такова, что обработке подвергаются не только данные сотрудников и специалистов, но и директоров и их партнеров. Соответственно, была разработана и внедрена система получения согласия партнеров на обработку персональных данных. Наибольшие трудности возникают с технической стороны защиты персональных данных. В чем же причина? Обработка персональных данных велась на многих компьютерах, не объединенных в локальную сеть (по объективным причинам). Теперь же возникла необходимость использования одной базы данных с организацией доступа по паролю, что влечет за собой изменение и расширение структуры локальной сети предприятия. Также, необходимо определить возможные каналы утечки информации и возможные угрозы информационной системе, построить модель угроз нарушителя, и уже на их основа-

нии строить модель защиты. Не стоит забывать, что еще один необходимый шаг в организации технической стороны защиты персональных данных – обязательная сертификация программного обеспечения для ИСПД, что также выливается в немалые суммы.

В **заключение** следует сказать, что, по нашему мнению, неоценимую помощь может оказать независимый аудит. В планах предприятия проведение такого мероприятия с помощью одного из интеграторов нашего региона, что позволит выявить уязвимые места, возможные каналы утечки информации и объективно оценить существующий режим информационной безопасности. Также ожидается, что такой аудит позволит добиться максимальной отдачи от средств, инвестируемых в создание и обслуживание системы безопасности.

Список литературы

1. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 25.07.2011) «О персональных данных».

2. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 06.04.2011, с изм. от 21.07.2011) «Об информации, информационных технологиях и о защите информации».

3. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (ред. от 19.07.2011).

4. Романец В. Ю. Защита информации в компьютерных системах и сетях // Электрон. дан. Режим доступа URL: http://www.proklondike.com (дата обращения: 30.01.2017).

5. Скиба В. Ю., Курбатов В. А. Руководство по защите от внутренних угроз информационной безопасности. – СПб.: Лань, 2008. – 320 с.

6. Хорев П. Б. Методы и средства защиты информации в компьютерных системах. – М.: Издательский центр «Академия», 2005. – 256 с.

Заречнева А. С.
Научный руководитель – преподаватель математики и информатики
Викторова Ю. В.
Колледж Стерлитамакского филиала
ФГБОУ ВО «Башкирский государственный университет»
Республика Башкортостан, г. Стерлитамак

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Бурное развитие информационных технологий во всех сферах общественной жизни определило информацию как стратегический ресурс государства, производительную силу и дорогой товар. Это не может не вызывать стремления государств, организаций и отдельных граждан получить преимущества за счет овладения информацией, недоступной оппонентам, а также за счет нанесения ущерба информационным ресурсам конкурента и защиты своих информационных ресурсов.

Очевидно, что **проблема** обеспечения информационной безопасности на всех уровнях может быть решена успешно только в том случае, если создана и функционирует комплексная система защиты информации, охватывающая весь жизненный цикл компьютерных систем от разработки до утилизации и всю технологическую цепочку сбора, хранения, обработки и выдачи информации. Не маловажным и **актуальным** здесь является вопрос криптографической защиты информации.

Целью исследования является изучение возможностей методов шифрования для защиты информации от несанкционированного доступа и достижения информационной безопасности в целом.

Для достижения цели исследования нами были выделены **задачи**:

- изучить различные методы криптографической защиты информации;
- выявить применимость данных методов на практике.

Под криптографической защитой информации понимается такое преобразование исходной информации, в результате которого она становится недоступной для ознакомления и использования лицами, не имеющими на это полномочий [1].

Известны различные подходы к классификации методов криптографического преобразования информации. По виду воздействия на исходную информацию методы криптографического преобразования информации могут быть разделены на четыре группы: шифрование, стеганография, кодирование и сжатие (рис. 1).

Процесс шифрования заключается в проведении обратимых математических, логических, комбинаторных и других преобразований исходной информации, в результате которых зашифрованная информация представляет собой хаотический набор букв, цифр, других символов и двоичных кодов. Для шифрования информации используются алгоритм преобразования и ключ. Как правило, алгоритм для определенного метода шифрования является неизменным. Исходными данными для алгоритма шифрования служат информация, подлежащая зашифрованию, и ключ шифрования. Ключ содержит управляющую информацию, которая определяет выбор

преобразования на определенных шагах алгоритма и величины операндов, используемые при реализации алгоритма шифрования.

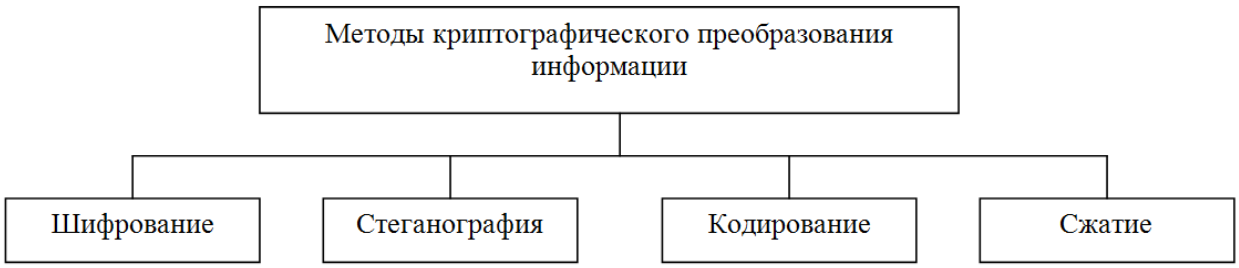


Рис. 1. Классификация методов криптографического преобразования информации

В отличие от других методов криптографического преобразования информации, методы стеганографии позволяют скрыть не только смысл хранящейся или передаваемой информации, но и сам факт хранения или передачи закрытой информации. В компьютерных системах практическое использование стеганографии только начинается, но проведенные исследования показывают ее перспективность [2].

Содержанием процесса кодирования информации является замена смысловых конструкций исходной информации (слов, предложений) кодами. В качестве кодов могут использоваться сочетания букв, цифр, букв и цифр. При кодировании и обратном преобразовании используются специальные таблицы или словари. С точки зрения целесообразности, кодирование информации применяется в системах с ограниченным набором смысловых конструкций.

Сжатие информации служит в первую очередь для сокращения объема информации и не относится к методам криптографического преобразования в строгом смысле. Сжатая информация не может быть прочитана или использована без обратного преобразования. На практике процесс сжатия файлов конфиденциальной информации совмещают с процессом шифрования.

Основным видом криптографического преобразования информации в компьютерных системах является шифрование, под которым понимается процесс преобразования открытой информации в зашифрованную информацию (шифртекст) или процесс обратного преобразования зашифрованной информации в открытую. Процесс преобразования открытой информации в закрытую получил название зашифрование, а процесс преобразования закрытой информации в открытую – расшифрование.

Исторически известно множество методов шифрования или шифров. Большинство из них не выдержали проверку временем, а некоторые используются и до сих пор. С появлением ЭВМ получил бурное развитие процесс разработки новых шифров, учитывающих возможности компьютеров как для зашифрования/расшифрования информации, так и для атак на шифр. Атака на шифр (криптоанализ) – это процесс расшифрования закрытой информации без знания ключа и, возможно, при отсутствии сведений об алгоритме шифрования.

Современные методы шифрования должны отвечать следующим требованиям:

– стойкость шифра противостоять криптоанализу (криптостойкость) должна быть такой, чтобы вскрытие его могло быть осуществлено только путем решения задачи полного перебора ключей;

– криптостойкость обеспечивается не секретностью алгоритма шифрования, а секретностью ключа;

– шифртекст не должен существенно превосходить по объему исходную информацию;

– ошибки, возникающие при шифровании, не должны приводить к искажениям и потерям информации;

– время шифрования не должно быть большим;

– стоимость шифрования должна быть согласована со стоимостью закрываемой информации.

Криптостойкость шифра является его основным показателем эффективности.

Все методы шифрования могут быть классифицированы по различным признакам (по типу ключей, по способу преобразования). По типу ключей выделяют методы шифрования с симметричным и открытым ключом.

Методы первого типа предполагают использование для зашифровывания и расшифровывания информации один и тот же секретный ключ. Среди них выделяют следующие:

– методы замены (подстановки), сущность которых заключается в замене символов исходной информации, записанных в одном алфавите, символами из другого алфавита по определенному правилу [3];

– методы перестановок, в основе которых лежит разделение исходного текста на блоки фиксированной длины и последующая перестановка символов внутри каждого блока по определенному алгоритму [3];

– аналитические методы, использующие для шифрования информации аналитические преобразования (наибольшее распространение получили методы шифрования, основанные на использовании матричной алгебры) [4];

– аддитивные методы, сущность шифрования которых заключается в последовательном суммировании цифровых кодов, соответствующих символам исходной информации, с последовательностью кодов, которая соответствует некоторому набору (кортежу) символов [3].

Методы второго типа (с открытым ключом) используют два ключа. Шифруется информация с помощью открытого ключа, а расшифровывается с использованием секретного ключа. В основе применения систем с открытым ключом лежит использование необратимых или односторонних функций [4]. Эти функции обладают следующим свойством. По известному x легко определяется функция $y = f(x)$. Но по известному значению y практически невозможно получить x. При шифровании с использованием открытого ключа нет необходимости в передаче секретного ключа между взаимодействующими субъектами, что существенно упрощает криптозащиту передаваемой информации. Криптосистемы с открытыми ключами различаются видом односторонних функций. Среди них самыми известными являются системы RSA, Эль-Гамаля и Мак-Элиса. В настоящее время наиболее эффективным и распространенным алгоритмом шифрования с открытым ключом является алгоритм RSA, получивший свое название от первых букв фамилий его создателей: Rivest, Shamir и Adleman.

Подводя **итог**, следует отметить, что для предотвращения угроз нарушения информационной безопасности важно знать существующие методы криптографии.

Список литературы

1. Завгородний В. И. Комплексная зашита информации в компьютерных системах: Учебное пособие. – М.: Логос; ПБОЮЛ Н. А Егоров, 2001. – 264 с.
2. Артехин Б. В. Стеганография // Защита информации. Конфидент. – 1996. – № 4.
3. Хоффман Л. Дж. Современные методы защиты информации / Пер. с англ. – М.: Сов. радио, 1980.
4. Герасименко В. А. Защита информации в автоматизированных системах обработки данных. – М.: Энергоатомиздат, 1994. – 352 с.

Исангулова Л. И.
Научный руководитель – преподаватель математики и информатики
Галикаева Л. А.
Колледж Стерлитамакского филиала
ФГБОУ ВО «Башкирский государственный университет»
Республика Башкортостан, г. Стерлитамак

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БАНКОВСКОЙ ДЕЯТЕЛЬНОСТИ

В наше время в связи с всеобщей информатизацией и компьютеризацией банковской деятельности значение информационной безопасности банков многократно возрастает. Актуальность темы заключается в том, что в банках сосредоточена важная и зачастую секретная информация о финансовой и хозяйственной деятельности многих людей, компаний, организаций и даже целых государств. Еще 30 лет назад объектом информационных атак были данные о клиентах банков или о деятельности самого банка. Такие атаки были редкими, круг их заказчиков был очень узок, а ущерб мог быть значительным лишь в особых случаях. Совершить попытку хищения может любой – необходимо лишь наличие компьютера, подключенного к сети Интернет. Причем для этого не требуется физически проникать в банк, можно «работать» и за тысячи километров от него.

Цель нашей работы: выявить угрозы, возникающие для банковской информации и основные методы её защиты от этих угроз.

Задачи:

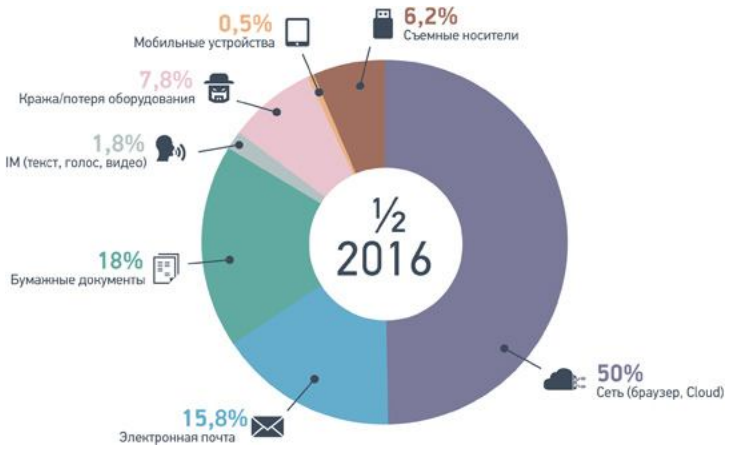
- дать классификацию угроз банковской информации;
- указать основные направления защиты банковской информации.

Ранее, когда все банковские операции совершались исключительно при помощи наличных средств, банкам угрожала лишь одна опасность: грабеж. Грабеж мог произойти в самом отделении банка либо при транспортировке денежных средств. На сегодняшний день угрозы стали более разнообразными.

Можно рассматривать следующую классификацию угроз банковской информации: 1) несанкционированный доступ – получение доступа к информационному ресурсу, на который у злоумышленника нет прав. Съем и получение информации в данном случае производится с применением специальной аудио или видео аппаратуры. Одной из со-

временных форм взлома является использование электрических и электромагнитных излучений, обеспечивающих злоумышленникам возможность получения конфиденциальной информации; 2) человеческий фактор является основной и главной угрозой информационной безопасности, напрямую зависящей от человеческих отношений. Большая часть утечки информации объясняется халатностью персонала банка, который оставляет важную информацию в доступном месте, например, привычка записывать имя или пароль на клочке бумаги, лежащем на столе, сотрудник банка может вынести носитель информации за пределы территории. По статистике, около 80 % правонарушений приходится на сотрудников банка, то есть на тех, кто непосредственно имел или имеет доступ к данным [2]; 3) вирусные атаки, то есть в результате действия, например, «троянского коня» возможно искажение, хищение, удаление критически важной информации; 4) распространение программного обеспечения, специализирующего на хищении паролей; 5) уничтожение информации в результате поломки программно-технического обеспечения, сбоями операционных систем.

Так, по данным компании InfoWatch, которая занимается разработкой решений для защиты бизнеса от внутренних угроз информационной безопасности в I полугодии 2016 года увеличились доли утечек информации по таким каналам, как съемные носители, электронная почта и снизились доли утечек данных в результате кражи/потери оборудования, через сеть, бумажные документы [5].



Анализируя список существующих угроз – можно определить основные направления защиты банковской системы:

1. Физическая защита, включает в себя защиту оборудования от механических повреждений, хищений, установки специального оборудования для электромагнитного съема, охрану и защиту зданий, помещений, компьютеров, перевозимых документов и т.п., обеспечение безопасности аппаратных средств.

2. Аутентификация пользователей позволяет защитить банковскую информацию от несанкционированного доступа, т.е. проверка правильности введенной пользователем регистрационной информации для входа в систему. Используется для принудительного применения избирательных прав доступа к информационным ресурсам и прав на выполнение операций в системе.

3. Антивирусная защита. Установка комплекса специализированного программного обеспечения по предотвращению проникновения в вычислительную сеть вредоносных программ.

4. Использование в компьютерных сетях брандмауэров. Брандмауэр – система, которая создающая защитный барьер между двумя или большим количеством сетей и предотвращающая вторжение в частную сеть, служат виртуальными барьерами для передачи пакетов из одной сети в другую.

5. Тщательный подбор сотрудников, распределение полномочий и построение системы допуска к элементам информации, а также контроль дисциплины и поведения сотрудников, создание хорошего морального климата в коллективе.

6. Правовой уровень защиты информации представлен нормативными документами для банков и финансовых учреждений. Это 161-ФЗ «О национальной платежной системе», 152-ФЗ «О персональных данных», 149-ФЗ «Об информации, информационных технологиях и о защите информации», стандарты Банка России серии СТО БР ИББС, международный стандарт индустрии платежных карт PCI DSS. Под охраняемой законом понимается информация, для которой законом установлен специальный режим ее правовой защиты (например, государственная, служебная и коммерческая тайна, персональные данные и т.д.).

Разработкой средства защиты банковской информации занимаются многие фирмы. В России, например, компания «Код Безопасности» предлагает полную линейку сертифицированных продуктов, благодаря которым будет обеспечена реальная защита информации в банках и финансовых учреждениях. Они разрабатывают средства защиты информации, предназначенное для обеспечения безопасности виртуальной инфраструктуры, системы защиты информации на серверах и рабочих станциях от несанкционированного доступа, защиту компьютера от сетевых вторжений, вредоносных программ и спама, обеспечивает защиту компьютера с применением межсетевого экрана, антивируса и средства обнаружения вторжений, аппаратно-программное средство защиты компьютера от несанкционированного доступа (аппаратно-программный модуль доверенной загрузки) и т.п. [3].

Итак, нами были рассмотрены угрозы, возникающие для банковской информации и основные методы для защиты этой информации. Финансовые учреждения обязаны принимать активные меры, позволяющие защитить конфиденциальную информацию от преступников. И как видно методов для этого достаточно. Банкам необходимо внимательно изучить рынок систем безопасности. Все подсистемы должны интегрироваться в существующую информационную систему и, желательно, иметь общее управление. В противном случае неминуемы повышенные трудозатраты на администрирование защиты и увеличение рисков из-за ошибок в управлении.

Список литературы

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

2. Альшанская Т. В. Применение методов системного анализа специалистами по информационной безопасности. Информационные системы и технологии: управление и безопасность: Сб. ст. III международной заочной научно-практической конференции / Поволжский гос. ун-т сервиса. – Тольятти: Изд-во ПВГУС, 2014. – 348 с.

3. Трофимова В. В. Информационные системы и технологии в экономике и управлении. – М.: Юрайт, 2012. – 521 с.

4. Трошина С. М. Расследование инцидентов информационной безопасности // «Юридический мир», 2016. – № 4. – С. 49–54.

5. https://www.infowatch.ru.

Истрафилов Т. Р.
Научный руководитель – преподаватель экономических дисциплин
Почанина Н. Х.
Колледж Стерлитамакского филиала
ФГБОУ ВО «Башкирский государственный университет»
Республика Башкортостан, г. Стерлитамак

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ В БАНКОВСКОЙ СФЕРЕ

Защита персональных данных в век информационных технологий стала особенно актуальной. Случаев, когда злоумышленники получают доступ к любой конфиденциальной информации, атакуя информационные системы организаций, становится всё больше. Несомненно, атаки не обходят стороной и банковскую сферу. Поскольку в банковских системах содержится большое число персональных данных клиентов, их безопасность должна находиться под пристальным вниманием государства и самих владельцев кредитно-финансовых учреждений.

Для начала стоит разобраться, что же это такое персональные данные? Какая информация может стать доступна банку, если он станет его клиентом?

В Федеральном законе «О персональных данных» дано четкое определение терминам «персональные данные», «обработка персональных данных».

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных [1].

Для начала рассмотрим вид информации, подлежащий защите в кредитной организации: 1) персональные данные: фамилия, имя и отчество; дата и место рождения; гражданство; место регистрации и фактического проживания; все данные паспорта (серия, номер, когда и кем выдан документ); номер мобильного и домашнего телефона; место работы, занимаемая должность; 2) банковская тайна; 3) коммерческая тайна.

Конечно, клиент надеется, что его персональные данные при обработке и хранении будут надежно защищены.

Для того чтобы кредитно-финансовые учреждения могли качественно организовать систему обработки и защиты персональных данных, необходимо обозначить перечень нормативно-правовых актов, на которые стоит опираться банку при работе с персональными данными клиентов [2, с. 423]:

1. Конституция Российской Федерации.
2. Трудовой кодекс РФ.
3. Гражданский кодекс.
4. Уголовный кодекс РФ.
5. Федеральный закон № 152 «О персональных данных».
6. Федеральный закон № 149 «Об информации, информационных технологиях и о защите информации».
7. Федеральный закон № 395-1 «О банках и банковской деятельности».

Так же в банках при создании системы обработки и хранения персональных данных создаётся ряд локальных документов, обеспечивающий дополнительный контроль для работы с данными.

Банковская организация при получении от клиента его персональных данных принимает на себя обязанность проводить все организационно-технические мероприятия по защите, доверенной ему информации от несанкционированного доступа (случайного или преднамеренного), блокирования, модификации, уничтожения и иных противоправных действий.

Рассмотрим реальные угрозы информации, обрабатываемой в банке: 1) вирусные атаки; 2) атаки на платежные карты; 3) сетевые атаки на сайты банков; 4) атаки на банкоматы и платежные терминалы; 5) инсайдерская деятельность сотрудников кредитной организации (использование информации, подделка документов, вброс фальшивых электронных платежей, путем атаки на ключи подписи, увод средств со счетов).

Стоит выделить ряд мер, для качественной организации обработки и защиты персональных данных в банках:

1. Назначение ответственных за обработку и обеспечение безопасности данных в информационной системе банка.

2. Осуществление мер контроля и ознакомление сотрудников с соответствующей нормативно-правовой базой и внутренними документами, на которых базируется система безопасности данных банка.

3. Определение угроз при обработке персональных данных в банке и мер их противодействию.

4. Оценка эффективности применяемых организационно- технических мер по обеспечению защиты данных, до введения системы защиты в эксплуатацию.

5. Учёт всех машинных носителей персональных данных.

6. Установление правил доступа к системе обработки и защиты для сотрудников.

7. В случае выявления несанкционированного доступа к защищаемым данным принятие мер по ликвидации угрозы и восстановление утерянных данных.

И обязательное мероприятие для банков с действующей системой хранения и защиты персональных данных клиента – постоянный контроль и совершенствование системы безопасности.

Таким образом, стоит отметить, что обработка, хранение и защита персональных данных в банках должна осуществляться на основании условий, определенных нормативно-правовой базой Российской Федерации. Каждая кредитно-финансовая организация должна:

- соблюдать принцип законности при организации защиты персональных данных своих клиентов;
- проводить полный комплекс мер по организационно-технической защите данных;
- при создании локальных документов, связанных с обеспечением информационной безопасности опираться на лучшие российские и международные практики в данной сфере;
- выполнять все требования контролирующих органов (ФСТЭК, Роскомнадзор, ФСБ) по обеспечению защиты персональных данных клиента.

Из интервью взятого электронной газетой «ВолгаНьюс» у директора Управления Регионального контактного центра одного из банков, зарегистрированных на территории РФ можно отметить несколько важных моментов [3]:

Во-первых, свои персональные данные по телефону можно сообщать только сотрудникам банка, обратившись по номеру горячей линии, для того, чтобы пройти процесс аутентификации. В противном случае, можно попасть в сети аферистов.

Во-вторых, банк рекомендует хранить квитанции устройств самообслуживания в течение шести месяцев. То же касается чеков об изъятии карты и технической ситуации банкомата в случае неуспешного взноса наличных денежных средств. Если клиенту необходима квитанция о подтверждении платежа, а чек утерян, необходимо обратиться в филиал банка за документом, подтверждающим платеж.

В-третьих, не стоит передавать третьим лицам, не имеющих отношение к банку, в котором обслуживается клиент, свои персональные данные.

Поэтому, в заключении хотелось бы отметить, несмотря на то, что банк принимает ряд мер по защите персональных данных своих клиентов, необходимо быть бдительным, при предоставлении своих личных данных.

Список литературы

1. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ.
2. Коробова Г. Г. Банковское дело. Учебник – М.: Инфра-М, 2015. – 592 с.
3. Дмитриенко А. А. Как клиенту банка защитить свои персональные данные. [Электронный ресурс] // Информационный портал Волга Ньюс. URL: http://volga.news/article/416487.html (дата обращения 15.01.2017).

Калимуллина С. К.
Научный руководитель – учитель истории и обществознания
Строчко Т. Н.
МБОУ «СОШ № 24 с углубленным изучением иностранного языка»
Республика Башкортостан, г. Салават

ВЛИЯНИЕ ВИРТУАЛЬНОГО ПРОСТРАНСТВА СЕТИ ИНТЕРНЕТ НА МИРОВОЗЗРЕНИЕ СОВРЕМЕННОЙ МОЛОДЁЖИ

Мировоззрение – целостное представление о природе, обществе, человеке, находящее выражение в системе ценностей и идеалов личности, социальной группы, общества [4].

Рассмотрим несколько особенностей мировоззрения. Во-первых, оно всегда исторично, то есть связано с совокупностью проблем, которыми непосредственно живет общество. Во-вторых, мировоззрение определяет общую направленность личности. В-третьих, оно всегда связано с убеждением. В-четвертых, мировоззрение отражается на всём облике человека, на его поведении, привычках, действиях и поступках. Поразмыслив, многие из нас смогут назвать составляющие представления о мире, коими являются знания, убеждения, принципы, духовные ценности, идеи и идеалы. Носителем мировоззрения может быть не только отдельная личность, но и социальная группа, общество в целом и даже человечество определенной эпохи. Остановимся на такой социальной группе как молодежь, которая представляет собой социально-демографическую группу, выделяемую на основе совокупности возрастных характеристик (приблизительно от 16 до 25 лет), особенностей социального положения и определенных социально-психологических качеств [1, с. 232].

Мы считаем, что подросток и социальная сеть – это одна из **актуальных тем** нашего времени, так как социализация человека происходит в процессе воспитания и под значительным влиянием среды, а которая в наше время существенно изменилась: обострилась ситуация влияния как глобальной сети, так и социальных сетей на подрастающее поколение. Некоторые считают, что это приносит пользу, некоторые – что вред. Таким образом, **проблемой нашего исследования** является влияние Интернета на современную молодёжь.

Нашей **целью** является изучение влияния виртуального пространства Интернет на мировоззрение современной молодёжи.

Перед собой мы поставили следующие **задачи**: проследить влияние Всемирной сети на мировоззрение подростков, раскрыть позитивные и негативные стороны социальных сетей на современную молодёжь и найти способы решения проблем, связанных с времяпровождением подростков в социальных сетях.

Нам кажется, что регулярное времяпровождение в Интернете вошло в привычку у современных юношей и девушек. Молодые люди чаще всего регистрируются в социальных сетях с целью повысить свое настроение, найти старых и новых друзей, всегда быть «в контакте». Существуют и другие, более целесообразные причины: работа, учёба, отдых, развлечения, Интернет-услуги и покупки. Необъятное виртуальное пространство привлекает все больше и больше людей, стремящихся найти информацию, удовлетворить потребности в общении, шопинге, развлечениях. Постепенно это приводит к зависимости от Всемирной паутины, торможению развития человека как личности, «зомбированию», ухода из реального мира: попадая в виртуальный мир, молодежь лихорадочно «блуждает» по сети, зачастую забывая о ежедневных делах, учебе и работе, о взятых на себя обязательствах, полностью «растворяясь» в манящих и красочных сайтах. В подобных случаях речь идет об Интернет-зависимости или так называемой Интернет-аддикции – непреодолимого желания подключиться к Интернету в режиме офлайн и неспособность завершить сеанс, находясь в режиме онлайн [2, с. 1344]. Многие люди, находясь в социальных сетях, не замечают, как быстро летит время и насколько они привязаны к потоку информации, насколько трудно выключить компьютер и обратить внимание на реальные предметы. Кроме того, длительное времяпровождение за компьютером отрицательно сказывается на здоровье высшей нервной деятельности, эндокринной, иммунной и репродуктивной системах; не в меньшей, а то и большей степени сказанное касается зрения и костно-мышечного аппарата человека [4].

Однако Интернет обладает массой достоинств, облегчающих повседневную жизнь современного человека. Всем известно, что глобальная сеть сближает общество на глобальном уровне: его используют для создания и развития бизнеса, для импорта и экспорта товаров, для отдыха и релаксации, поиска данных и любой информации, то есть для мировой торговли и коммуникации. Систематизируем безусловные плюсы Интернет-пространства: электронная почта, доступ к информации, покупки, онлайн-общение, сообщества, бизнес, сферы услуг.

По мнению немецкого социолога первой половины XX века, Карла Маннгейма, молодежь есть потенция, готовая к любому начинанию. Молодые люди всегда по-своему воспринимали ценности культуры, что порождало в разные времена молодёжный сленг и различные формы субкультуры (хиппи, готы, стиляги и т.п.) Рассмотрим подробнее роль Интернета в формировании мировоззрения у молодёжи, обратившись к структуре мировоззрения. Интернет содержит колоссальное количество информации, а, следовательно, благодаря своей популярности и распространенности является важным источником получения знаний. Так, по данным опроса фонда «Общественное мнение» на 2016 год, в качестве положительных сторон интернета 60 % опрошенных отметили – «много полезной и общедоступной информации». Социальные сети не только способствуют расширению круга общения за счет собеседд-

ников из других городов, районов и даже стран, но и часто позволяют наблюдать за интересами, принципами, убеждениями и мировоззрением в целом конкретного пользователя сети, значит, появляется возможность подчерпнуть какие-то идеи, найти идеал. Например, поклонники какого-либо художника могут следить за жизнью своего кумира, посещая (виртуально в данном случае) его аккаунты в социальных сетях, и вдохновляться его творчеством. Однако стоит отметить, что в Интернете отсутствуют ограничения в получении любого рода информации. Бесконтрольность доступа к ресурсам глобальной сети таит в себе серьезные потенциальные опасности для человека, а особенно для молодых людей, у которых ещё наблюдается активный процесс социализации. В Интернете содержится большое количество ресурсов, демонстрирующих и пропагандирующих различные формы насилия, популяризирующих различные методы манипуляции сознанием, насаждающих мистицизм, расизм, нацизм, конкретные религии и т.п. Как пишет современный публицист Сергей Черкасов: «Сегодня многие молодые люди, живущие в разных странах, увлекшись идеями радикального ислама, продолжают попытки проникнуть к боевикам ИГ на Ближнем Востоке». И здесь наблюдается связь с глобальной сетью: «Вербовка начинается с интернета – там ищут потенциальных жертв».

Благодаря наличию практически повсеместного доступа к Интернету, многие молодые люди предпочитают искать информацию с помощью ПК или смартфона, вместо того чтобы спросить у товарища, то есть Всемирная паутина фактически заменяет реальных людей виртуальностью. Одним из последствий становится неполнота элементов мировоззрения: мироощущение, мировосприятие и миропонимание складываются на основе жизни в Интернете. По мнению французского ученого Жана-Франсуа Руэ из Университета Пуатье, огромная масса информации в Глобальной сети нарушает ее восприятие у некоторых людей: «Пользователю приходится постоянно спрашивать себя, где находится эта информация, потому что он видит ее не как осязаемый перед собой, а как изображение на экране компьютера». Также, он считает, что подросткам свойственно наивное восприятие информации, полученной в Интернете, они не задумываются о ее достоверности и тем более не проверяют её. Так как я сама подросток, то довольно часто становлюсь свидетелем подобных ситуаций, в которых мои сверстники бездумно верят любому высказыванию и иной информации, найденной в Глобальной сети.

Таким образом, Интернет оказывает значительное влияние на ценностные ориентиры молодежи, он плотно вошел в обиход современного человека, грань между виртуальностью и реальностью стала очень тонкой. Недостаточно социализированные и слабые характером личности попадают под «волны» веб-пространства, полностью погружаясь в разнообразные сайты, социальные сети, чаты, форумы, онлайн-игры. Подобный «сёрфинг» приводит к негативным последствиям, влияя на мировоззрение подрастающего поколения: для молодого человека приоритетными становятся личные интересы, параллельно формируется безразличное отношение к обществу, социальным нормам и базовым общечеловеческим ценностям, таким как позитивное межличностное общение, сотрудничество, взаимопомощь. Постепенно обесценивается живое полноценное общение, реальный коммуникативный акт с его непосредственными эмоциями заменяется бесчувственными сухими сообщениями, чтение книг – сомнительной информацией поисковых сайтов, психологическое здо-

ровье – зависимостью от IT-технологий и виртуального информационного пространства в гаджетах и ПК.

В качестве **решения данной проблемы** следует принять законы, согласно которым будут заблокированы сайты, содержащие контент насильственного характера, а также пропаганду терроризма; учащимся на уроках информатики и обществознания рассказывать о вреде длительного времяпровождения в Интернете на здоровье и развитие человека как личности, о существовании недостоверных источников информации в Глобальной сети; студентам и родителям школьников раздавать памятки с правилами безопасного пользования сети Интернет [3, с. 35]; родители школьников должны ограничивать количество времени, которое их дети проводят за ПК.

Список литературы

1. Баранов П. А., Воронцов А. В., Шевченко С. В. Обществознание. Справочник. – 2016. – С. 232.

2. Патрикеева Э. Г., Соловьева О. А., Селезнева Т. А. Влияние виртуального пространства сети Интернет на жизненные ценности современной молодежи // Молодой ученый. – 2015. – № 10. – С. 1344.

3. Хорев П. Б. Методы и средства защиты информации в компьютерных системах. – М.: Издательский центр «Академия», 2005. – 256 с.

4. Электронная энциклопедия. // Электрон. дан. Режим доступа URL https://ru.wikipedia.org/wiki/ (дата обращения 28.01.2017).

Калкаманова Д. Р.
Научный руководитель – преподаватель экономических дисциплин
Абрамова Л. Н.
Колледж Стерлитамакского филиала
ФГБОУ ВО «Башкирский государственный университет»
Республика Башкортостан, г. Стерлитамак

ЭКОНОМИЧЕСКАЯ ИНФОРМАЦИЯ КАК ПРЕДМЕТ ЗАЩИТЫ

В современном обществе высока роль информационной сферы, которая представляет собой совокупность информации, осуществляющей сбор, формирование, распространение и использование информации. Она является главным фактором общественной жизни и влияет на многие составляющие части безопасности Российской Федерации.

Безопасность информации – это состояние сохранности информационных ресурсов государства, которая обеспечивает конфиденциальность, целостность и доступность информации. [3, с.10].

Можно выделить следующие виды угроз безопасности информации:

1) утечка информации;
2) угроза искажений (дезинформация, подделка, повтор);
3) угроза уничтожения информации;

4) угроза интеллектуальной собственности (незаконное копирование, воспроизведение и т.д.);

5) помехи функционирования информационных систем;

6) телекоммуникации (отказ от получения, отправления информации).

Одна из важнейших разновидностей информации – экономическая информация, возникающая в процессе производственно-хозяйственной деятельности, обслуживающая процессы производства, распределения и потребления материальных благ.

Наиболее важными характеристиками экономической информации можно назвать:

1) корректность (информация, обладающая содержанием, которое обеспечивает ее четкое восприятие всеми потребителями);

2) ценность (свойство информации, которое отражает, в какой степени она способствует достижению целей и задач ее потребителя);

3) достоверность (отражение некоторой объективной реальности с самой реальностью);

4) точность (определяется мерой близости (удаленности) их друг от друга);

5) актуальность (степень соответствия информации текущему моменту времени);

6) полнота (отражает достаточность информации или недостаточность для принятия управленческого решения).

Для того чтобы защитить информацию существуют методы защиты экономической информации – это методы, которые предотвращают утечку информации и ее потерю.

Основными методами защиты считаются:

1) управление доступом (методы защиты информации регулированием использования всех ресурсов информационной системы и информационных технологий);

2) препятствие (метод физического преграждения пути злоумышленнику к защищаемой информации);

3) механизмы шифрования (криптографическое закрытие информации);

4) регламентация (создание условий автоматизированной обработки, хранения и передачи защищаемой информации, при которых нормы и стандарты по защите выполняются в наибольшей степени);

5) принуждение (метод защиты, при котором пользователи и персонал информационной системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности);

6) побуждение (метод защиты, побуждающий пользователей и персонал информационной системы не нарушать установленные порядки за счет соблюдения сложившихся моральных и этических норм).

Информация является изначально слабозащищенным ресурсом, и поэтому представляется чрезвычайно важным принимать повышенные меры ее защиты, соблюдая полный комплекс обеспечения информационной безопасности.

Защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб собственнику, владельцу, пользователю и иному лицу. Наряду с этим защита информации распространяется и на сведения, от-

несенные к государственной тайне, на конфиденциальную документированную информацию и в отношении персональной информации.

На федеральном уровне принимаются следующие меры для обеспечения информационной безопасности: осуществляется формирование и реализация единой государственной политики по обеспечению защиты национальных интересов от угроз в информационной сфере, устанавливается баланс между потребностью в свободном обмене информацией и допустимыми ограничениями ее распространения, совершенствуется законодательство РФ в сфере обеспечения информационной безопасности, а также, унифицируются средства поиска, сбора, хранения, обработки и анализа информации для вхождения в глобальную информационную инфраструктуру. [1, ст. 5]

Защита данных в компьютерных сетях становится одной из самых открытых проблем в современных информационно-вычислительных системах. Рассматривая проблемы, связанные с защитой данных, возникает вопрос о классификации сбоев и несанкционированности доступа, что ведет к потере или нежелательному изменению данных. Это могут быть сбои оборудования (кабельной системы, дисковых систем, серверов, рабочих станций и т.д.), потери информации (из-за инфицирования компьютерными вирусами, неправильного хранения архивных данных, нарушений прав доступа к данным), некорректная работа пользователей и обслуживающего персонала. Перечисленные нарушения работы в сети вызвали необходимость создания различных видов защиты информации. Условно их можно разделить на три класса:

1) средства физической защиты;

2) программные средства (антивирусные программы, системы разграничения полномочий, программные средства контроля доступа);

3) административные меры защиты (доступ в помещения, разработка стратегий безопасности фирмы и т.д.).

Универсального решения, исключающего причины, которые могут серьёзно повлиять на работу локальных и глобальных сетей или привести к потере ценной информации, нет, однако во многих организациях разработаны и применяются технические и административные меры, позволяющие риск потери данных или несанкционированного доступа к ним свести к минимуму.

Список литературы

1. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ, принят госдумой от 08.07.2006 г.

2. Смирнов А. А. Обеспечение информационной безопасности в условиях виртуализации общества. Опыт Европейского Союза: монография. – ЮНИТИ-ДАНА. Закон и право, 2012 г. – 196 с.

3. Блинов А. М. Информационная безопасность. – 2013. – 96 с.

Лаврентьев В. С.
Научный руководитель – учитель начальных классов
Лаврентьева М. А.
МБОУ «СОШ № 24 с углубленным изучением иностранного языка»
Республика Башкортостан, г. Салават

СОЦИАЛЬНЫЕ СЕТИ И МОЛОДЁЖЬ: ЗА ИЛИ ПРОТИВ?

Современную жизнь невозможно представить без Интернета. Всемирная сеть открывает перед человечеством широчайшие возможности: дополнительного заработка, онлайн-покупок, нахождения нужной и интересной информации, учёбы и повышения квалификации посредством скачивания из сети не только разнообразных учебников, но и дипломных работ, научных статей и даже диссертаций, записи онлайн на приём к врачу, просмотр видео, прослушивание и скачивание музыки. Но, пожалуй, одним из широко используемых преимуществ является возможность онлайн – общения между людьми, находящимися в разных точках земного шара.

В последнее время среди людей всех возрастов, а особенно молодежи особой популярностью пользуется общение в сети. Любой человек может найти себе подходящий способ общения в виртуальном пространстве.

Очень распространённой формой компьютерного общения является электронная почта (Е-мэйл). Ею пользуются в основном для деловой переписки или пересылки документов различных форматов.

Для молодёжи большой привлекательностью обладают социальные сети, благодаря которым существует возможность неформального общения.

Актуальность данной темы заключается в том, что социальных сетей становится всё больше. По статистике примерно половина всех россиян зарегистрированы в социальных сетях, а многие в нескольких сразу. Согласно мнению отечественных ученых, 98 % подростков общаются через Интернет. Неоднозначность влияния социальных сетей на подростков вызывает интерес к изучению этой проблемы.

Цель работы: определить степень влияния социальных сетей на современную молодежь (в частности учащихся МБОУ «СОШ № 24» г. Салавата).

Задачи:

- провести анкетирование среди учащихся школы, чтобы выяснить цели их виртуального общения и степень его влияния на них;
- проанализировать ответы учащихся и представить результаты в виде диаграмм;
- сделать необходимые выводы и отразить их в данной работе.

В России самыми популярными на сегодняшний день являются в «Вконтакте» (86 %), «Одноклассники» (75 %), Facebook (58 %) [2, с. 40]. Молодёжь не представляет своей жизни без ежедневного посещения социальных сетей, черпает информацию из лент новостей интернет-сайтов, общается через комментарии, оценивает фотографии друг друга, дарит подарки и открытки. Это удобный способ общения различных социальных групп: одноклассников, студентов, однокурсников, друзей, коллег. На своей странице можно разместить и просмотреть фотографии, музыку, ви-

деоролики. В социальной сети каждый может высказать своё мнение как открыто, так и анонимно. Можно зарегистрироваться под своим именем и общаться не таясь, а можно, наоборот, не открывая своего лица и настоящего имени. Неуверенных в себе часто привлекает и такая возможность. Подростки также пользуются ею из хулиганских побуждений.

Но есть и большой минус. У молодёжи в последнее время очень развита привязанность к телефону и плееру. Многие подростки просто не выпускают их из рук, стараясь занять себя не только в свободное время, но и в учебное, что не приносит ничего, кроме вреда.

В статье К. Янга «Диагноз – Интернет-зависимость» приводится статистика по данным опроса. Она свидетельствует о том, что около 54 % зависимых от интернета не собираются уменьшать своё времяпровождение в сети, при этом зная, что это наносит вред их здоровью и психике. Часть из них думают, что уже не смогут избавиться от этой вредной привычки. Остальные 46 % пытались избавиться от зависимости, но безуспешно. Сначала они пробовали ограничить время, которое можно было проводить в интернете, но контролировать самих себя они были не в состоянии, затем выбрасывали модемы, резали провода, но через некоторое время снова оказывались в сети, осознавая, что без Интернета они не могут [4, с. 23].

Группа ученых под руководством профессора Пола Киршнера провела исследование, целью которого было выяснить влияние социальных сетей на успеваемость студентов. Всего в эксперименте приняли участие 219 учащихся в возрасте от 19 до 54 лет [2, с. 39].

Итоги оказались следующими. Студенты, которые на время подготовки к экзаменам полностью отказались от Интернет-общения, показали результат на 20 % лучше остальных. Если средняя оценка по четырехбалльной шкале у любителей социальных сетей составила 3,06, то те, кто накануне сессии расстался с Интернетом, показали результат в 3,82 балла.

«Если Facebook и другие социальные сети работают в фоновом режиме, а человек занят более важной работой, ему приходится отвлекаться и переключать свое внимание, что приводит к появлению большого числа ошибок в выполняемой работе», – заявил Киршнер [2, с. 39].

Подобный результат не стал неожиданностью для профессора. Он уверен, что цифры будут точно такими же, если провести исследование среди школьников. Тем не менее, настаивает Киршнер, он не собирается демонизировать общение в социальных сетях – все хорошо в меру.

Мы провели социологическое исследование среди учащихся 7–11 классов нашей школы. По результатам анкетирования выяснилось, что 100 % учащихся посещают социальные сети. Это можно увидеть на рис. 1.

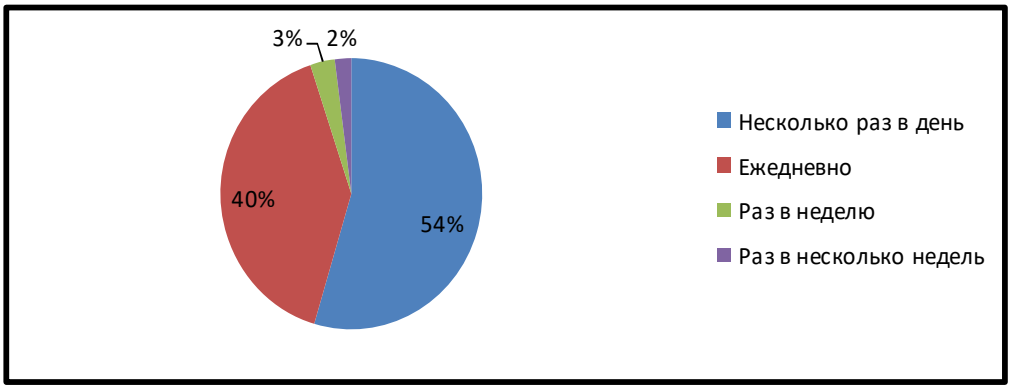


Рис. 1. Частота посещения социальных сетей

Основными мотивами для использования социальных сетей для них являются поиск друзей, одноклассников, однокурсников и общение с ними.

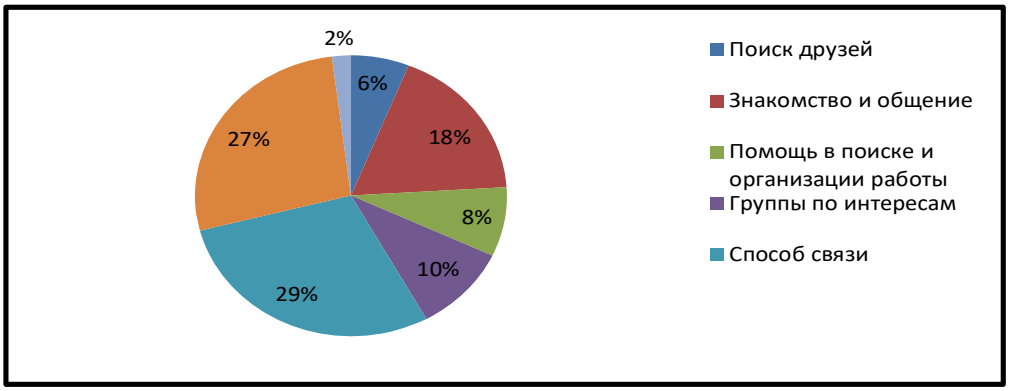


Рис. 2. Мотивы посещения социальных сетей

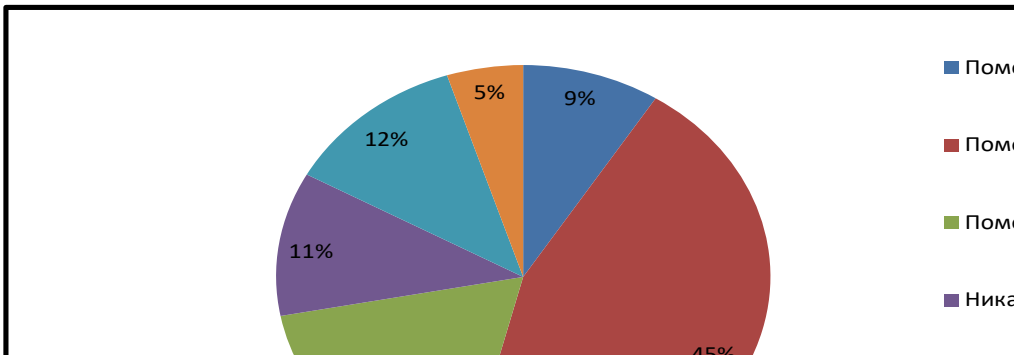


Рис. 3. Влияние социальных сетей на образ жизни

Приоритетным в использовании услуг, предоставляемых социальной сетью для школьников является возможность найти интересующую их музыку, фильмы, фото, поиск и обмен информации, а также способ связи, экономящий средства и время.

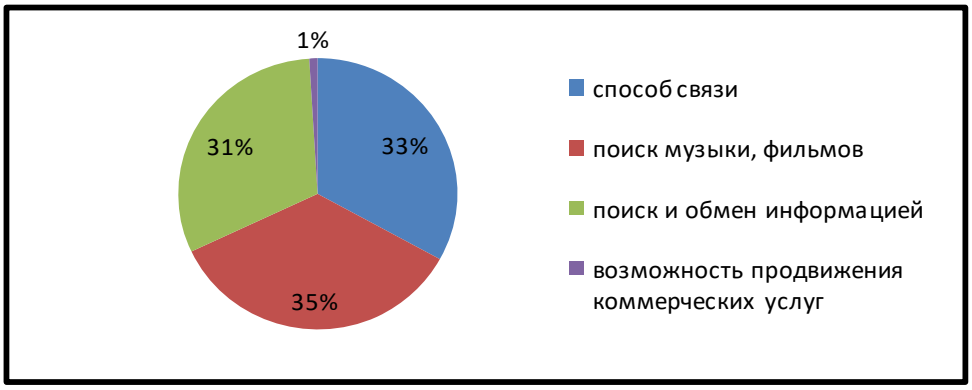


Рис. 4. Приоритетные услуги, предоставляемые социальной сетью

1 % школьников зарабатывает с помощью социальных сетей.

55 % не признают тот факт, что социальные сети негативно влияют на их успеваемость, остальные согласны с этим фактом.

84 % считают возможным появление зависимости человека от социальных сетей.

Подводя **итоги**, следует заметить, что социальные сети, став неотъемлемой частью полноценной жизни школьника, заняли большую часть его свободного времени. Подросткам они заменяют хобби, живое общение. В то же время дети не считают, что социальные сети отвлекают их от важных дел, а наоборот уверены, что те помогают им сделать эту самую жизнь намного проще и интереснее.

Несмотря на то, что в виртуальном общении есть свои плюсы, следует отметить, что социальные сети чаще всего плохо влияют на учебу, хотя и бывают исключения. Поэтому следует контролировать количество времени, которое тратится на Интернет. Важно знать границу и не переходить её, иначе это обернется против тебя. Всегда помните известную поговорку: всё хорошо в меру.

Список литературы

1. Ученые заявили о вреде социальных сетей. Ежедневная электронная газета Утро.ru [Электронный ресурс]. http://www.utro.ru/articles/2010/09/08/9207 44.shtml (дата обращения 28.01.2017).

2. Шумакова Е. В. Воспитательное пространство социальных сетей интернета // Профессиональное образование. Столица. – 2011. – № 6. – С. 39–40.

3. Электронный математический и медико-биологический журнал. – Т. 10. – Вып. 2. – 2011. – URL: http://www.smolensk.ru/user/sgma/MMORPH/N-30-html/cont.htm (дата обращения 27.01.2017).

4. Янг К. Диагноз – Интернет-зависимость [Электронный ресурс]. URL: http://www.narcom.ru/publ/info/665 (дата обращения 27.01.2017).

Максутова Д. А.
Научный руководитель – преподаватель математики и информатики
Галикаева Л. А.
Колледж Стерлитамакского филиала
ФГБОУ ВО «Башкирский государственный университет»
Республика Башкортостан, г. Стерлитамак

ИНТЕРНЕТ-ЗАВИСИМОСТЬ – ПРОБЛЕМА СОВРЕМЕННОГО ОБЩЕСТВА

Интернет очень прочно вошел в нашу жизнь, многие просто не представляют себе без него жизнь. Едва оказавшись в доступном для Интернета месте, они первым делом заходят на любимые сайты, узнают новости, «общаются» с друзьями, комментируют, просматривают, скачивают. Безусловно, информация имеет для человека огромное значение, она формирует личность, но бывает, что она, же и разрушает ее. **Актуальность** нашего исследования заключается в том, что, сегодня подростки – пользователи Интернета чрезмерно увлечены всемирной паутиной, что иногда разрушающе действует на их психику.

Целью данной работы стало раскрытие понятия зависимости от Интернета, выяснение признаков ее возникновения.

Задачами нашей работы является выяснение причин Интернет-зависимости и способами решения данной проблемы.

Интернет-зависимость – психическое расстройство, навязчивое желание подключиться к Интернету и болезненная неспособность вовремя отключиться от Интернета. Все формы зависимости, в том числе и Интернет-зависимости, характеризуются поиском чувства удовлетворения, в данном случае – при использовании Интернета. В результате увеличивается время, которое затрачивается на достижение этого чувства. При этом отсутствие Интернета может быть равносильно стрессовой ситуации.

Впервые расстройство было описано в 1995 году доктором Иваном Голдбергом. Несмотря на то, что в цели Голдберга не входило включение этого расстройства в официальные психиатрические стандарты, предложенное им описание базируется на описании расстройств, связанных со злоупотреблением психоактивными веществами. Голдберг выделил следующие основные симптомы этого расстройства:

– использование Интернета вызывает болезненное негативное стрессовое состояние или дистресс;

– использование Интернета причиняет ущерб физическому, психологическому, межличностному, экономическому или социальному статусу.

В 1997–1998 гг. были созданы исследовательские и консультативно-диагностические службы по данной проблематике. В 1998–1999 гг. вышли первые монографии по проблеме (К. Янг, Д. Гринфилд и др.). В России данный феномен изучается в основном психологами. Интерес представляют работы психиатра Виталины Буровой, которая первая из российских врачей начала серьёзно изучать данное явление. Согласно ее исследованиям выделяют следующие формы Интернет-зависимости: зависимость от компьютерных игр (гейм-аддикция), зависимость от се-

тевых действий (Интернет-аддикция), зависимость от криминальных действий с помощью компьютера (хаккинг и другие виды криминального программирования).

Проблема Интернет-зависимости выявилась с возрастанием популярности сети Интернет. Некоторые люди стали настолько увлекаться виртуальным пространством, что начали предпочитать Интернет реальности, проводя за компьютером до 18 часов в день. Резкий отказ от Интернета вызывает у таких людей тревогу и эмоциональное возбуждение. Многие люди считают Интернет-зависимость сходной с химической зависимостью вроде курения или наркомании. Психиатры же усматривают схожесть такой зависимости с чрезмерным увлечением азартными играми.

Официально медицина пока не признала Интернет-зависимость психическим расстройством, и многие эксперты в области психиатрии вообще сомневаются в существовании Интернет-зависимости или отрицают вред от этого явления.

Зависимость в медицинском смысле определяется как навязчивая потребность в использовании привычного вещества, сопровождающаяся ростом толерантности и выраженными физиологическими и психологическими симптомами. Но в случае с Интернет-зависимостью никакого «привычного вещества» в прямом смысле слова не существует.

Поэтому характер зависимости иной, чем при употреблении наркотиков или алкоголя, то есть физический компонент полностью отсутствует. А вот психологический проявляется очень ярко. Таким образом, можно определить Интернет-зависимость как нехимическую зависимость – навязчивую потребность в использовании Интернета, сопровождающуюся социальной дезадаптацией и выраженными психологическими симптомами.

По данным различных исследований, Интернет-зависимыми сегодня являются около 10 % пользователей во всём мире. Российские психиатры считают, что сейчас в нашей стране таковых 4–6 %. Несмотря на отсутствие официального признания проблемы, Интернет-зависимость уже принимается в расчёт во многих странах мира.

Основные 5 типов Интернет-зависимости:

– навязчивый веб-серфинг – бесконечные путешествия по Всемирной паутине, поиск информации;

– пристрастие к виртуальному общению и виртуальным знакомствам – большие объёмы переписки, постоянное участие в чатах, веб-форумах, социальных сетях, избыточность знакомых и друзей в Сети;

– игровая зависимость – навязчивое увлечение компьютерными играми по сети;

– навязчивая финансовая потребность – игра по сети в азартные игры, ненужные покупки в Интернет-магазинах или постоянные участия в Интернет-аукционах;

– киберсексуальная зависимость – навязчивое влечение к посещению порносайтов и занятию киберсексом.

Анализ показывает, что главенствующим фактором, благодаря которому все эти явления получили широкое распространение, является анонимность личности в Интернете.

Проблемы в семье, как правило, возникают в результате недостатка внимания к тому или иному члену семьи. Ссоры и непонимание проблем зависимого человека только усугубляют положения отношения в семье. Лучший способ решить проблемы семьи это любовь и взаимопонимание, и мудрость домочадцев. Плавно выводить че-

ловека на семейное позитивное общение и главное увеличивать совместное общение с живой природой, возможно, это прогулки.

Надо отметить, что по сравнению с зависимостями от алкоголя и наркотиков, Интернет-зависимость в меньшей степени вредит здоровью человека, не разрушает его мозг и казалась бы достаточно безопасной, если бы не явное снижение трудоспособности, эффективности функционирования в реальном социуме. Как наркотик, общение в Интернете может создавать иллюзию благополучия, кажущуюся возможность решения реальных проблем. Хотя, как показывают исследования Московских психологов, многие Интернет-зависимые отдают себе отчет в том, что не получат реальной поддержки в сети, и не расценивают Интернет как среду, гарантирующую общение.

Интернет стал более «легким» наркотиком и шансом избавиться от более серьезных зависимостей. Известны алкоголики и наркоманы, которые сократили злоупотребление вредными веществами, а многие и вовсе отказались от них, благодаря многочасовым сессиям в Сети. То есть, они заместили одну зависимость на другую. По такому же принципу работают многие методы психотерапевтического лечения зависимостей: заместить вредную привычку на более «экологичную», безопасную.

Также, Интернет-зависимость является более «экологичной» по сравнению с зависимостями от религиозных сект, где людьми откровенно манипулируют с целью установления власти и материальной наживы. Известно, что участники этих религиозных движений, ежемесячно должны жертвовать определенные суммы денег, они постепенно утрачивают собственную волю и сходят с ума. Так, что религиозный культ является в данном случае маскарадом, скрывающим истинные намерения руководителей. В секты тоже попадают зависимые, внушаемые люди.

Итак, благодаря своим качествам: анонимности, доступности, невидимости, безопасности, простоты использования, Интернет оказывает неоценимую услугу людям, страдающим от вредных привычек, предоставляя им возможность отказаться от последних, и в то же время может наносить вред подросткам и молодежи, которые вместо социализации в реальном мире, находят возможность социализации в мире виртуальном.

Многих людей, столкнувшихся с Интернет-зависимостью, интересует вопрос, как с ней бороться. Можно прибегнуть к советам психологов, которые знают, как избавиться от Интернет-зависимости.

1. Уделять несколько часов в день на выполнение физических упражнений или работы по дому. Неважно, что это будет за занятие, главное чтобы мышцы получали нагрузку, тем самым способствуя улучшению работы сердца и кровеносной системы.

2. День без Интернета. В этот день можно делать все, что угодно: гулять, читать, встретиться с друзьями, но не включать компьютер.

3. Путешествовать. Дорога способствует знакомству с новыми местами и людьми.

4. Читать книги не менее одного часа в день. Человек сам отдает предпочтение виду литературе. Нужно помнить, что чтение дает возможность обогатиться и выглядеть в глазах окружающих мудрее.

Придерживаясь данных рекомендаций, больше не возникнет вопроса относительно того, как побороть интернет зависимость. Лучше всего уделять больше времени со знакомством с чем-то новым, привить себе желание учиться и развиваться, а не сидеть каждый день перед монитором.

Итак, резюмируя выше сказанное, на вопрос «Где выход из данной проблемы?» можно дать ответ «По большому счету там же, где и вход». Главная цель – зависимому человеку необходимо вернуться в реальную жизнь. Для этого подойдет все, что нравится, увлекает, вызывает позитивные чувства. У кого-то это спорт, у других – творчество, увлекательная работа, хобби, любовь. В этом нелегком процессе важна поддержка близких людей, а при необходимости и психологическая помощь.

Список литературы

1. Коптелова Н. И. Интернет-зависимость среди подростков как психолого-педагогическая проблема // Научно-методический электронный журнал «Концепт». – 2016. – Т. 11. – С. 3101–3105.

2. Лотякова А. М. Феномен Интернет-зависимости у подростков // Гуманитарные научные исследования. – Декабрь. – 2016.

3. Максс В. А. Компьютерная зависимость у подростков // Молодой ученый. – 2014. – № 7. – С. 272–274.

4. Панкова Т. В., Сергеева Н. В. Исследование Интернет-зависимости подростка // Современная педагогика. – Май. – 2014.

5. Пахомова Т. В. Некоторые психологические проблемы Интернет-зависимости // Молодой ученый. – 2014. – № 15. – С. 236–238.

Малышева К. А.
Научный руководитель – преподаватель экономических дисциплин
Абрамова Л. Н.
Колледж Стерлитамакского филиала
ФГБОУ ВО «Башкирский государственный университет»
Республика Башкортостан, г. Стерлитамак

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ЭКОНОМИЧЕСКОЙ ИНФОРМАЦИИ

Информация является одним из наиболее ценных ресурсов любой компании, поэтому обеспечение защиты информации является одной из важнейших и приоритетных задач. Безопасность информационной системы – это свойство, заключающее в способности системы обеспечить ее нормальное функционирование, то есть обеспечить целостность и секретность информации. Для обеспечения целостности и конфиденциальности информации необходимо обеспечить защиту информации от случайного уничтожения или несанкционированного доступа к ней.

Обеспечить безопасность информации можно различными методами и средствами, как организационного, так и инженерного характера. Комплекс организационных мер, программных, технических и других методов и средств обеспечения безопасности информации образует систему защиты информации.

К основным методам, которые используются при защите экономической информации, можно отнести следующие: скрытие, ранжирование, дезинформация, дробление, кодирование, шифрование, страхование [1, с. 76].

Скрытие как метод защиты экономической информации является в основе своей реализации на практике одним из основных организационных принципов защиты информации – максимального ограничения числа лиц, допускаемых к секретам. Реализация этого метода достигается обычно путем засекречивания информации и ограничения в связи с этим доступа к этой информации в зависимости от ее важности для собственника.

Ранжирование как метод защиты экономической информации является частным случаем метода скрытия и включает в себя, во-первых, деление засекречиваемой информации по степени секретности, и, во-вторых, регламентацию допуска и разграничение доступа к защищаемой информации: предоставление индивидуальных прав отдельным пользователям на доступ к необходимой им конкретной информации и на выполнение отдельных операций. Разграничение доступа к информации может осуществляться по тематическому признаку или по признаку секретности информации и определяется матрицей доступа.

Дезинформация заключается в распространении заведомо ложных сведений относительно истинного назначения каких-либо объектов и изделий, действительного состояния какой-то области государственной деятельности, положение дел на предприятии и т.д. Дезинформация обычно проводится путем распространения ложной информации по различным каналам, имитацией или искажением признаков и свойств отдельных элементов объектов защиты, создания ложных объектов, по внешнему виду или проявлениям похожих на интересующие соперника объекты и др.

Дробление (расчленение) экономической информации на части с таким условием, что знание какой-то одной части информации не позволяет восстановить всю технологию в целом. Применяется достаточно широко при производстве средств вооружения и военной техники, а также при производстве товаров народного потребления.

Кодирование – метод защиты экономической информации, преследующий цель скрыть от соперника содержание защищаемой информации и заключающийся в преобразовании с помощью кодов открытого текста в условный при передаче информации по каналам связи, направлении письменного сообщения, когда есть угроза, что он может попасть в руки конкурента, а также при обработке и хранении информации. Для кодирования используются обычно совокупность знаков (символов, цифр и др.) и система определенных правил, при помощи которых информация может быть преобразована (закодирована) таким образом, что прочитать ее можно будет, если потребитель располагает соответствующим ключом (кодом) для ее раскодирования.

Шифрование – метод защиты экономической информации, используемый при передаче сообщений с помощью различной радиоаппаратуры, направлении письменных сообщений и в других случаях, когда есть опасность перехвата этих сообщений соперником. Шифрование заключается в преобразовании открытой информации в вид, исключающий понимание его содержания, если перехвативший не имеет сведений (ключа) для раскрытия шифра. Шифрование может быть предварительное (шифруется текст документа) и линейное (шифруется разговор). Для шифрования информации может использоваться специальная аппаратура.

Страхование как метод защиты информации сводится к тому, чтобы защитить права и интересы собственника информации или средства информации как от тради-

ционных угроз (кражи, стихийные бедствия), так и от угроз безопасности информации, а именно: защита информации от утечки, хищения, модификации (подделки), разрушения и др.

Страховые методы защиты информации будут применяться, прежде всего, для защиты коммерческих секретов от промышленного шпионажа. Особенно страховые методы будут эффективны в независимом секторе экономики, где административные методы и формы управления, а особенно контроля, плохо применимы. При страховании информации должно быть проведено аудиторское обследование и дано заключение о сведениях, которые предприятие будет защищать как коммерческую тайну, и надежности средств защиты.

Средства защиты информации – это совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, а также иных материальных элементов, используемых для решения различных задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации. Инженерно-технические средства включают в себя: фильтры, экраны на аппаратуру, ключ для блокировки клавиатуры, устройства аутенфикации – для чтения отпечатков пальцев, формы руки, радужной оболочки глаза, скорости и приемов печати [2, с. 65].

Статистика показывает, что во всех странах убытки от злонамеренных действий непрерывно возрастают. Причем основные причины убытков связаны с недостаточностью средств безопасности как таковых и с отсутствием взаимосвязи между ними. Для осуществления полноценной защиты информации необходима слаженная работа всех средств безопасности. Лишь в комплексе они могут обеспечить полноценную защиту ценных данных. Поэтому необходимо опережающими темпами совершенствовать комплексные средства защиты.

Естественно, что указанные средства защиты не всегда надежны, так как на сегодняшний день быстрыми темпами развивается не только техника (в нашем случае компьютерная), постоянно совершенствуется не только сама информация, но и методы, позволяющие эту информацию добывать.

Список литературы

1. Батурин Ю. М., Жодзинский А. М. Компьютерная преступность и компьютерная безопасность. – М.: Юридическая литература, 2016. – 160 с.

2. Ярочкин В. И. Система безопасности фирмы – М.: Академия, 2013. – 178 с.

Марахотин А. А.
Научный руководитель – преподаватель юридических дисциплин
Аракелян Л. К.
Колледж Стерлитамакского филиала
ФГБОУ ВО «Башкирский государственный университет»
Республика Башкортостан, г. Стерлитамак

ЗАВИСИМОСТЬ МОЛОДЕЖИ ОТ СОЦИАЛЬНЫХ СЕТЕЙ – БОЛЕЗНЬ XXI ВЕКА

Зависимость современной молодежи от социальных сетей является важной и **актуальной**, сложной социальной проблемой, обусловленной тем, что для многих виртуальное пространство становится второй реальностью, где проводится большая часть сознательной жизни, воспринимается большой поток информации сомнительного содержания, происходит общение и знакомство, в том числе несовершеннолетних, с совершенно незнакомыми лицами различных возрастов, преследующие не всегда благие цели, искажается реальность, пользователи подвержены сильному идеологическому влиянию.

Цель данного исследования – выявить причины и условия, способствующие формированию зависимости современной молодежи от социальных сетей, а также пути ее решения.

Для достижения поставленной цели необходимо решить следующие **задачи исследования**: 1) рассмотреть процесс становления и развития социальных сетей; 2) определить причины и условия, способствующие формированию зависимости современной молодежи от социальных сетей; 3) составить модель последствия рассматриваемой зависимости; 4) сформировать пути решения рассматриваемой проблемы исследования.

Процесс формирования рассматриваемой зависимости у современной молодежи стал предметом научного исследования сравнительно недавно и нашел отражение в немногочисленных работах таких отечественных и зарубежных ученых, как: Бэлл Даниэл, Элвин Тоффлер и т.д. [1, с. 5].

Первая в мире социальная сеть появилась в США в 1995 году и называлась «Classmates.com» («Одноклассники» являются его русским аналогом), что вызывало настоящий ажиотаж среди людей различных слоев и возрастов [6]. Как того и следовало ожидать, со временем бум социальных сетей охватил весь мир.

Целью социальных сетей изначально была консолидация людей по интересам, а также упрощение общения между ними на любом расстоянии. Как следствие, существование возможности отправлять мгновенные сообщения в сети одному или нескольким людям одновременно стало значительно экономить время и средства. Так социальные сети стали привлекать внимание предпринимательского сектора: организации, а также индивидуальные предприниматели получили возможность рекламировать свои товары, услуги и работы благодаря наличию возможности создавать так называемые группы.

Суждение о том, что общение в группах социальных сетей не приводит к положительным результатам, является довольно спорным. С помощью них можно манипулировать людьми, реализовывать мошеннические проекты, растлевать молодежь и многое другое. Но в то же время каждый может научиться отстаивать свою точку зрения и аргументировать ее, делиться различной информацией. Подобные группы очень удобны для студенческой молодежи, ведь благодаря им всегда можно узнать новости университета, колледжа, курса, группы, расписание или задания по предметам [1, с. 5].

Многие социальные сети, например, «Фэйсбук» [9], «В Контакте» [7], «Твиттер» [8], позволяют быть в курсе событий, происходящих в жизни «друзей», в муниципальном образовании, регионе, стране и мире в целом.

В социальных сетях участились так называемые «фейковые аккаунты», которые используют не всегда с безобидной целью. Находящаяся на странице информация может оказаться ложью. Однако человеческое любопытство берет верх, поэтому молодые люди засиживаются допоздна, стараясь не упустить обновление новостей, и постепенно впадают в своеобразную зависимость. Подобный феномен чреват отрешением от внешнего мира, дезориентацией в реальной жизни. Человеку становится дискомфортно вне сети, поэтому он снова включает свой гаджет и начинает проверять обновления новостей и свои сообщения, вместо того, чтобы провести время вместе с родными и близкими, реальными друзьями, узнать, как у них дела не по статусам, а при непосредственном вербальном общения.

Недаром Аристотель сказал, что «наслаждаться общением – главный признак дружбы» [7, с. 137]. Элвин Тоффлер в своей книге «Третья волна», вышедшей в свет ещё в 1980 году подчеркнул, что «дети будущих поколений будут расти в обществе, которое гораздо меньше сосредоточено на ребенке. «Поседение» или постарение населения во всех высокоразвитых странах предполагает, что общество уделяет больше внимания потребностям пожилых людей и, соответственно, меньше – молодым. Далее, по мере того как женщины продвигаются по службе и делают карьеру в рыночной экономике, их традиционная потребность тратить все свои силы на материнство уменьшается» [10, с. 285].

Таким образом, молодым людям не хватает внимания и должной заботы со стороны старших, поэтому они закрываются от всех в своем собственном виртуальном мире, становятся «заложниками» собственного виртуального мира.

Последствия зависимости от социальных сетей могут довольно пагубно отразиться на становлении и развитии многих поколений, на демографической ситуации в стране. Такого рода зависимость будет чревата психологическими расстройствами, замкнутостью, нежеланием, а, возможно, и страхом перед общением с реальными людьми вне сети. В случае подобного развития событий психолог станет самой популярной профессией.

Зависимость молодежи от социальных сетей – это бич современного общества. Люди все чаще стали «уходить» с помощью использования специальных психотропных препаратов, наркотического опьянения, из мира реальных проблем в мир иллюзий, с помощью виртуальной реальности «растворять» существующие проблемы. Это, в свою очередь, приводит к еще большим сложностям. Как отмечает О. И. Елхова, «человек теряет ориентацию уже и в реальном мире и оказывается неспособным уви-

деть грань, разделяющую реальную жизнь и ее электронный фантом» [5, с. 67]. Увеличение количества социальных сетей («Вконтакте», «Одноклассники», «Facebook», «Twitter» и т.д.), возникших с целью создания возможностей организовывать вокруг себя единомышленников, организации общения, послужили одной из причин возникновения все более возрастающей проблемы современного мира – проблемы одиночества, когда «кажущиеся на первый взгляд привлекательными новые возможности в конечном результате оборачиваются бытием среди обезличенных других. В итоге, углубляясь в общение с Das Man человек оказывается окруженным многочисленными короткими, пустыми и взаимозаменяемыми виртуальными отношениям» [5, с. 67]. Людям необходимо использовать социальные сети целесообразно и при необходимости, поэтому нужно всем научиться вовремя, нажать кнопку «выйти».

Таким образом, можно предложить следующие **пути решения рассматриваемой проблемы исследования**:

1) на федеральном уровне принять нормативно-правовой акт, в полной мере регламентирующий правовой статус собственников, создателей и работников социальных сетей, порядок регистрации и осуществления деятельности социальных сетей;

2) установить строгую процедуру регистрации с обязательным заполнением персональных данных, контактных данных, а также приложением копии документа, удостоверяющего личность;

3) ввести административную ответственность организации за несвоевременное или не в полной мере ограничение доступа к контенту, содержащему информацию экстремистского или иного растлевающего характера в социальной сети;

4) на федеральном уровне принять нормативно-правовой акт, закрепляющий запрет на пользование социальными сетями учащимися образовательных учреждений под угрозой дисциплинарного взыскания со стороны образовательного учреждения;

5) Правительству РФ возложить на Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций обязанности по контролю за исполнением вышеуказанных нормативно-правовых актов, а также за установлением и использованием специальных технических средств и файерволов, ограничивающих доступ к социальным сетям в образовательных учреждениях;

6) усилить контроль и надзор за деятельностью социальных сетей, в том числе за публикуемым и используемым контентом.

Список литературы

1. Аракелян Л. К. Проблема зависимости молодёжи от социальных сетей // Вестник СМУС74. – 2014. – № 1. – С. 5–6.

2. Белл Д. Грядущее постиндустриальное общество. – М.: Академия, 2004. – 940 с.

3. Вараксин А. В. Влияние социальных сетей на формирование ценностных ориентиров современной молодежи // Преподаватель XXI век. – 2016. – № 2. – С. 205–212.

4. В контакте. Популярная социальная сеть. URL: http://www.vk.com (дата обращения 05.02.2017).

5. Елхова О. И. Виртуальная реальность коммуникации. // Известия РГПУ имени А. И. Герцена. – 2010. – № 137. – С. 66–67.

6. Классмейтс. Популярная социальная сеть. URL: http://www. classmates.com (дата обращения 05.02.2017).

7. Спиркин А. Г. Философия. – М.: Юрайт, 2010. – 832 с.
8. Твитттер. Популярная социальная сеть. URL: http://www.twitter.com (дата обращения 05.02.2017).
9. Фейсбук. Популярная социальная сеть. URL: http://www.facebook.com (дата обращения 05.02.2017).
10. Тоффлер Э. Третья волна. – М.: АСТ, 2004. – 781 с.

Мельникова А. М.
Научный руководитель – преподаватель математики и информатики
Викторова Ю. В.
Колледж Стерлитамакского филиала
ФГБОУ ВО «Башкирский государственный университет»
Республика Башкортостан, г. Стерлитамак

ВИРУСЫ КАК УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Вредоносные программы: компьютерные вирусы, черви, троянские программы представляют собой серьезную угрозу информационной безопасности компьютерных систем.

Предотвратить проникновение вредоносного программного кода в информационные системы практически невозможно, если не обладать специальными знаниями в области антивирусной защиты. Даже при использовании самых современных антивирусных программ проблемы с вирусами могут возникать не только у обычных пользователей компьютеров, но и у системных администраторов.

Именно поэтому вопросы специальной теоретической и практической подготовки специалистов в области антивирусной защиты имеют особое значение и остаются всегда **актуальными**, так как темп развития информационных технологий постоянно увеличивается.

Целью исследования является изучение влияния компьютерных вирусов и других вредоносных объектов на информационную безопасность.

Для достижения цели исследования нами были выделены **задачи**:

– изучить различные способы распространения вредоносных программных объектов, основанных на использовании файлов программ и документов, загрузочных областей дисков и внешних носителей информации, каналов электронной почты и ресурсов Интернета;

– выявить каким образом компьютерные вирусы и другие вредоносные объекты могут воздействовать на компьютерные системы;

– рассмотреть способы обнаружения и методики удаления вредоносных объектов, применяемых в современных антивирусных программах.

Для успешной борьбы с компьютерными вирусами и другими вредоносными программными объектами необходимо четко представлять особенности связанных с ними угроз для информационной безопасности.

В связи с тем, что существует множество вредоносных программ, специалисты по информационной безопасности используют различные подходы к классификации вредоносных программ [1]: по типам вредоносных программ; по степени распространенности; по вредоносному воздействию; по уровню опасности. Среди основных типов вредоносных программ исследователи выделяют следующие [2]: компьютерные вирусы, черви, логические бомбы, троянские объекты, программы Backdoor, программные средства для получения несанкционированного доступа к компьютерным системам.

Важно отметить, что существует множество комбинированных вредоносных программ, сочетающих в себе различные свойства.

Рассмотрим более детально существующие компьютерные вирусы и их классификацию.

Список различных типов вирусов достаточно большой:

– файловый вирус, записывающий свой код в тело программного файла или офисного документа, который получает управление при запуске зараженной программы;

– загрузочный вирус, записывающий свой код в главную загрузочную запись Master Boot Record диска или внешнего накопителя информации;

– файлово-загрузочный вирус, представляющий собой комбинацию файлового и загрузочного вирусов;

– стелс-вирус, оставляющий в памяти компьютера модули, перехватывающие обращение программ к дискам;

– шифрующийся вирус – это вирус, который при заражении новых файлов и системных областей диска шифрует собственный код, пользуясь для этого случайными паролями (ключами);

– полиморфный вирус – это такой шифрующийся вирус, который при заражении новых файлов и системных областей диска шифрует собственный код, так что бы он отличался от созданного экземпляра;

– макрокомандный вирус, прикрепляется к файлам офисных документов и распространяется вместе с ними;

– почтовый вирус использует для своего распространения каналы электронной почты;

– вирус в пакетном файле операционной системы (ОС) который записывает свое тело внутрь пакетного файла ОС, маскируя исполнимый код под строки комментариев;

– вирус в драйверах ОС, внедряющийся в файлы драйверов ОС;

– бестелесный вирус заражает только оперативную память компьютера, не попадая в файлы или служебные области дисков;

– вирус для пиринговых (файлообменных) сетей – это вредоносная программа, специально предназначенная для систем обмена файлами между компьютерами пользователей Интернета;

– комбинированный вирус, в котором реализована комбинация нескольких существенно различных методов или алгоритмов заражения, а также распространения;

– коллекционный вирус, который существует только в коллекциях вирусов специалистов и компаний, занимающихся профессиональной разработкой антивирусных программ.

Знание особенностей вирусов различных типов важно не только для разработки антивирусных программ, но и для их грамотного использования.

Среди известных методов обнаружения вирусов и других вредоносных программ, выделяют следующие:

– сканирование;
– эвристический анализ;
– обнаружение изменений;
– анализ сетевого трафика;
– анализ баз данных почтовых программ;
– обнаружение вирусов в системе автоматизации документооборота;
– вакцинирование.

Большинство вирусов и вредоносных программ не только размножаются, они еще выполняют вредоносные действия, предусмотренные их автором.

У разных вирусов эти дополнительные действия могут быть опасными или неопасными, бросающимися в глаза или скрытыми, трудно обнаружимыми. Рассказать обо всех проявлениях вирусов невозможно, так как для этого придется описать каждый вирус.

Подробную информацию о вредоносных воздействиях вирусов можно найти в вирусных базах данных, размещенных на Web-сайтах разработчиков антивирусного программного обеспечения.

Мы будем классифицировать вредоносные действия по их воздействию и эффектам:

– визуальные и звуковые эффекты, многообразие которых ограничено только фантазией разработчика;

– воздействие на файлы путем изменения хранящейся в них информации, атрибутов файла (имя, дата создания, размер, режим доступа и т.д.), переименования и удаления их;

– воздействие на базы данных, выполняя над ней операции по изменению и удалению хранящейся в базе данных информации;

– воздействие на аппаратное обеспечение компьютера, в виде имитации повреждения оборудования компьютера таким образом, чтобы создалось впечатление о необходимости ремонта или замены;

– получение несанкционированного доступа и похищение информации через предоставление злоумышленнику полный удаленный доступ к отдельным пораженным компьютерам и даже ко всей системе в целом;

– компрометация пользователя и социальный инжиниринг (провоцирование пользователя), когда вредоносная программа может воспользоваться хранящейся на компьютере персональной информацией для выполнения от имени пользователя каких-либо действий его компрометирующих.

Не все вирусы обладают явно выраженными вредоносными действиями. Однако даже те вирусы, которые не совершают вредоносных действий, могут представлять опасность из-за ошибок, допущенных авторами вирусов.

Современные антивирусные программы реализуют многие из перечисленных выше методов обнаружения вирусов и других вредоносных программ.

При сканировании антивирусная программа просматривает содержимое файлов, расположенных на дисках компьютера, а также содержимое оперативной памяти компьютера с целью поиска вирусов. Метод сканирования позволяет обнаружить такие вредоносные программы, которые не используют для противодействия антивирусным программам шифрование своего программного кода. При использовании метода, основанного на обнаружении изменений, вызываемых вирусами и вредоносными программами в файлах, антивирус контролирует все выполняемые программой действия, отслеживая при этом потенциально опасные, характерные для вирусов. Однако эвристический анализ не дает полной гарантии обнаружения любых новых вирусов, и в тех случаях, когда программа выполняет какие-либо действия, характерные для вирусов, может принять «безобидную» программу за вредоносную.

Следует отметить, что сегодня наибольшую угрозу представляют собой вирусы и другие вредоносные программы, распространяющиеся по каналам электронной почты. Наиболее эффективной методикой обнаружения и нейтрализации вредоносных программ, распространяющихся по каналам электронной почты, является анализ трафика электронной почты непосредственно на почтовом сервере.

Современные антивирусные программы позволяют пользователям, не обладающим очень высокой квалификацией, эффективно бороться с компьютерными вирусами и другими вредоносными программами. После удаления вредоносного кода из файла его состояние, как правило, не может быть восстановлено в точности. Это может привести к неработоспособности «вылеченных» программ и повреждению файлов офисных документов. Иногда антивирус не в состоянии удалить из файла тело вируса.

Подводя итог, следует отметить, что для предотвращения угроз нарушения информационной безопасности очень важно знать существующие виды вирусов и уметь применять возможности современных антивирусных программ для их нейтрализации.

Список литературы

1. Михайлов А. В. Компьютерные вирусы и борьба с ними. – СПб.: Диалог-МИФИ, 2011. – 104 с.

2. Гошко С. В. Технологии борьбы с компьютерными вирусами: – СПб.: Солон-Пресс, 2009. – 352 с.

3. Пилюгин П. Л. Общие вопросы зашиты вычислительных систем и особенности защиты персональных компьютеров: Курс лекций. – М.: ИКСИ, 1997. – 84 с.

Сабитова Э. А.
Научный руководитель – преподаватель экономических дисциплин
Абрамова Л. Н.
Колледж Стерлитамакского филиала
ФГБОУ ВО «Башкирский государственный университет»
Республика Башкортостан, г. Стерлитамак

ИНТЕЛЛЕКТУАЛЬНАЯ СОБСТВЕННОСТЬ ПРЕДПРИЯТИЯ И ЕЕ ЗАЩИТА

Интеллектуальная собственность – это закрепленная законодательством исключительные права на результат интеллектуальной деятельности. Эти законы устанавливают некую монополию авторов на результаты интеллектуальной и творческой деятельности, тем самым, другие лица могут пользоваться ими только с разрешения тех, кому принадлежит эта собственность.

Интеллектуальная собственность в наше время один из дорогостоящих активов предприятий, особенно, если предприятия получают большую выгоду не от производственных мощностей, а от доходов от патентов, товарных знаков и других нематериальных активов.

Наличие объектов интеллектуальной собственности можно зафиксировать практически на каждом предприятии. К ним относятся: изобретения, полезные модели, промышленные образцы, товарные знаки, наименования мест происхождения товара, селекционные достижения, фирменное наименование, коммерческие обозначения, секреты производства (ноу-хау) и т.д.

В современной экономике доля нематериальных активов, представленных, в основном, объектами интеллектуальной собственности, составляет более 50 % в составе имущественного комплекса предприятия (в развитых странах этот показатель, как правило, варьируется в пределах 60–70 %)

Учитывая тот факт, что интеллектуальная собственность – это совокупность прав и обязанностей отдельных лиц в представленной сфере, государство обеспечивает юридическую охрану этой категории. Для создания грамотной стратегии защиты интеллектуальной собственности необходимо знать, какие существуют нарушения. На сегодняшний день можно выделить ряд следующих нарушений [1, с. 112]:

- нарушение авторских прав (пиратство и плагиат);
- распространение или использование объектов, которые содержат методы, описанные или содержащиеся в патентах;
- ввоз на территорию Российской Федерации контрафактного товара;
- любые действия, направленные на обход существующих способов защиты авторских и смежных прав, а также распространение объектов для этих целей;
- изменение или подделка информации, которая имеет интеллектуальную ценность или связана с результатами интеллектуальной деятельности;
- нарушения прав на географическое обозначение товаров.

Следует отметить, что в каждой стране существует специальная служба по интеллектуальной собственности, которая занимается вопросами защиты данной категории, а также в некоторых случаях рассматривает споры по факту нарушения прав граждан. Существует три способа правовой охраны интеллектуальной собственности: в режиме авторского права, патентного права и коммерческой тайны.

Выбор способа правовой охраны предопределяется спецификой самого охраняемого результата интеллектуальной деятельности. Так, например, произведения науки, литературы и искусства – это объекты авторского права, которое защищает не содержание, а форму произведения. Право на защиту в этом случае возникает в момент создания нового продукта, независимо от государственной регистрации результата интеллектуальной деятельности, хотя добровольная регистрация объектов авторских прав по законодательству возможна. Под объекты авторского права подпадают, в том числе программы для ЭВМ и базы данных.

Патентное право, объекты которого – изобретения, полезные модели и промышленные образцы,– связывает защиту такой интеллектуальной собственности с обязательной государственной регистрацией и получением охранного документа – патента.

Федеральная служба по интеллектуальной собственности (РОСПАТЕНТ) является федеральным органом исполнительной власти, осуществляющим функции по регистрации прав интеллектуальной собственности, контролю и надзору в сфере правовой охраны и использования объектов интеллектуальной собственности, патентов и товарных знаков и результатов интеллектуальной деятельности, вовлекаемых в экономический и гражданско-правовой оборот, соблюдения интересов Российской Федерации, российских физических и юридических лиц при распределении прав на результаты интеллектуальной деятельности, в том числе создаваемые в рамках международного научно-технического сотрудничества [2, с. 126].

Третий способ – защита в режиме коммерческой тайны – подразумевает регистрацию охраняемых результатов интеллектуальной деятельности внутри компании и соблюдение норм закона о коммерческой тайне. Это могут быть секреты производства и изобретательские ноу-хау. Режим коммерческой тайны отличается от патентной охраны тем, что информация об охраняемом патентом результате интеллектуальной деятельности открыто, публикуется и доступна всем заинтересованным лицам. В то же время патент запрещает изготовление продукта, в котором использован запатентованный объект, на территории действия патента.

Также российская и международная интеллектуальная собственность могут охраняться посредством правовых норм, предусматривающих использование специальных графических обозначений, фиксирующих факт защиты объекта творческого труда авторским правом. Например, это может быть легко узнаваемый значок копирайта или, например, товарного знака, который зарегистрирован в установленном порядке.

Защита и оспаривание прав по интеллектуальной собственности осуществляется в следующих инстанциях: в суде по интеллектуальным правам, Роспатенте, в палате по патентным спорам, арбитражном суде.

Таким образом, управление интеллектуальной собственностью в России осуществляется за счёт деятельности службы, в структуру которой входят специальные подведомственные организации, имеющие специфические задачи и функции. Итак, в

статье мы рассмотрели понятие интеллектуальной собственности, основные аспекты и виды данной подотрасли гражданского права, а также организации интеллектуальной собственности. Следует отметить тот факт, что данная сфера развивается все сильнее с каждым днём. Поэтому особенности правового регулирования интеллектуальной собственности являются наиболее приоритетными среди учёных-практиков сегодня.

Список литературы

1. Батурин Ю. М. Интеллектуальная собственность как ценный объект предприятия – М.: Юридическая литература, 2015. – 212 с.

2. Ярочкин В. И. Система безопасности фирмы – М.: Академия, 2013. – с. 178.

Синельникова А. А.
Научный руководитель – учитель истории и обществознания
Аблеева Н. В.
МБОУ «СОШ № 24 с углубленным изучением иностранного языка»
Республика Башкортостан, г. Салават

СОВРЕМЕННЫЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ ОТ КИБЕРУГРОЗ

Развитие новых информационных технологий и всеобщая компьютеризация привели к тому, что информационная безопасность становится обязательной. Существует довольно обширный класс систем обработки информации, при разработке которых фактор безопасности играет первостепенную роль.

В последнее время эксперты в целом ряде стран отмечают увеличение целенаправленных компьютерных атак на системы управления критически важными объектами экономики.

Среди них – энергосистемы, АЭС и другие предприятия атомной промышленности, банки, линии связи, а также транспортные коммуникации. Поэтому надёжная информационная защита ключевых отраслей экономики становится важнейшим фактором обеспечения безопасности всего государства. Касается это и транспортной инфраструктуры.

По данным журнала «PC World» в 2011 г. число сложных и направленных атак увеличилось на 81 %, а исследование компании Verizon за 2012 г. показало, что произошло 855 случаев нарушения информационной безопасности, в результате чего под угрозой оказались 174 млн. записей

Данная тема **актуальна**, так как развитие современных информационных технологий характеризуется постоянным повышением уровня значения информации. Далее мы будем рассматривать **проблему** пагубного влияния киберугроз на информационные системы.

Цель работы: получение полного всестороннего анализа методов защиты информации.

Задачей является исследование существующих методов защиты информации от киберугроз.

Лавинообразный рост самых различных киберугроз делает сегодня задачу обеспечения информационной безопасности в малом и среднем бизнесе актуальной как никогда.

В настоящее время все киберугрозы принято разделять на внешние и внутренние. Причины и источники внешних угроз находятся вне компьютеров компании, как правило, в глобальной сети. Внутренние угрозы зависят исключительно от персонала компании, программного обеспечения и оборудования.

Наиболее опасными вирусами является кибероружие, которое направлено в некоторых случаях на уничтожение промышленной инфраструктуры.

Вторым по важности типом киберугроз является спам. В настоящее время доля спама в общем объеме электронной корреспонденции может достигать 70 %. Все это приводит к финансовым потерям. Помимо этого, спам также является одним из распространенных каналов внедрения троянских программ и вирусов.

Большую опасность представляет также удаленный взлом компьютеров, за счет которого злоумышленники, находящиеся, возможно, на другом конце планеты, могут получать возможность читать и редактировать документы, хранящиеся на файл-серверах и компьютерах, по собственному желанию уничтожать их, внедрять собственные программы, которые будут следить за всеми действиями конкурентов и собирать определенную информацию, вплоть до незаметного аудио- и видеонаблюдения через микрофоны ноутбуков и штатные веб-камеры.

На сегодняшний день все вышеперечисленные киберугрозы являются основными. Вполне очевидно, что для осуществления полноценной защиты информационного пространства компании, систем обработки данных и хранения информации необходимо не просто установка соответствующего программного обеспечения, но целый комплекс административно-организационных, программно-технических и нормативно-правовых мероприятий. Очень важно при этом обеспечить защиту информации, носителей и устройств при помощи программного обеспечения и технических средств, создать нормативные документы, которые будут регламентировать порядок работы персонала с информацией, а также разработать комплекс мер, которые будут препятствовать утечке информации или доступу к ней неуполномоченных лиц.

Технологии защиты данных основываются на применении современных методов, которые предотвращают утечку информации и ее потерю. Сегодня используется пять основных способов защиты: 1) препятствие; 2) маскировка; 3) управление; 4) регламентация; 5) принуждение.

Все перечисленные методы нацелены на построение эффективной технологии защиты информации, при которой исключены потери по причине халатности и успешно отражаются разные виды угроз.

Под препятствием понимается способ физической защиты информационных систем, благодаря которому злоумышленники не имеют возможность попасть на охраняемую территорию.

Маскировка – способы защиты информации, предусматривающие преобразование данных в форму, непригодную для восприятия посторонним и лицами. Для расшифровки требуется знание принципа.

Управление – способы защиты информации, при которых осуществляется управление над всеми компонентами информационной системы.

Регламентация – важнейший метод защиты информационных систем, предполагающий введение особых инструкций, согласно которым должны осуществляться все манипуляции с охраняемыми данными.

Принуждение – методы защиты информации, тесно связанные с регламентацией, предполагающие введение комплекса мер, при которых работники вынуждены выполнять установленные правила. Если используются способы воздействия на работников, при которых они выполняют инструкции и поэтическим и личностным соображениям, то речь идет о побуждении.

Способы защиты информации предполагают использование определенного набора средств. Для предотвращения потери и утечки секретных сведений используются следующие средства:

- физические;
- программные и аппаратные;
- организационные;
- законодательные.

Физические средства защиты информации предотвращают доступ посторонних лиц на охраняемую территорию. Основным и наиболее старым средством физического препятствия является установка прочных дверей, надежных замков, решеток на окна. Для усиления защиты информации используются пропускные пункты, на которых контроль доступа осуществляют люди (охранники) или специальные системы. С целью предотвращения потерь информации также целесообразна установка противопожарной системы. Физические средства используются для охраны данных, как на бумажных, так и на электронных носителях.

Программные и аппаратные средства – незаменимый компонент для обеспечения безопасности современных информационных систем. Аппаратные средства представлены устройствами, которые встраиваются в аппаратуру для обработки информации. Программные средства – программы, отражающие хакерские атаки. Также к программным средствам можно отнести программные комплексы, выполняющие восстановление утраченных сведений. При помощи комплекса аппаратуры и программ обеспечивается резервное копирование информации – для предотвращения потерь.

Организационные средства сопряжены с несколькими методами защиты: регламентацией, управлением, принуждением. К организационным средствам относится разработка должностных инструкций, беседы с работниками, комплекс мер наказания и поощрения. При эффективном использовании организационных средств работники предприятия хорошо осведомлены о технологии работы с охраняемыми сведениями, четко выполняют свои обязанности и несут ответственность за предоставление недостоверной информации, утечку или потерю данных.

Законодательные средства – комплекс нормативно-правовых актов, регулирующих деятельность людей, имеющих доступ к охраняемым сведениям и определяющих меру ответственности за утрату или кражу секретной информации.

Криптография в цифровых технологиях необходима как инструмент защиты конфиденциальных данных, а так же как средство противодействия незаконному ко-

пированию и распространению данных, являющихся интеллектуальной собственностью. В настоящее время она рассматривается как средство защиты конфиденциальных данных от: 1) несанкционированного прочтения; 2) преднамеренного нарушения целостности либо уничтожения; 3) нежелательного копирования; 4) фальсификации.

Основные направления использования криптографических методов – передача конфиденциальной информации по каналам связи (например, электронная почта), установление подлинности передаваемых сообщений, хранение информации (документов, баз данных) на носителях в зашифрованном виде.

Процесс криптографического закрытия данных может осуществляться как программно, так и аппаратно. Аппаратная реализация отличается существенно большей стоимостью, однако ей присущи и преимущества: высокая производительность, простота, защищенность и т.д. Программная реализация более практична, допускает известную гибкость в использовании.

Криптографические методы защиты являются самыми надежными, так как защищается сама информация, а не доступ к ней. На сегодняшний день возможны два варианта реализации криптографического закрытия информации – программная и аппаратная.

Исходя из всего выше сказанного, мы приходим к **выводу**, что главное при определении мер и принципов защиты информации это квалифицированно определить границы разумной безопасности и затрат на средства защиты, а так же поддержание системы в работоспособном состоянии.

Список литературы

1. Килясханов И. Ш., Саранчук Ю. М. Информационное право в терминах и понятиях: Учебное пособие. Юнити-Дана. – 2011. – 135 с.

2. Кобб М., Джост М. Безопасность IIS. ИНТУИТ. – 2006. – 678 с.

3. Хорошко В. А, Чекатков А. А. Методы и средства защиты информации. – К.: Юниор, 2003. – 504 с.

4. Ященко В. В. Введение в Криптографию. – М.: МЦНМО, 2005. – 288 с.

Тапорина В. В.
Научный руководитель – к.п.н., преподаватель математики и информатики
Трошкина Е. Ю.
Колледж Стерлитамакского филиала
ФГБОУ ВО «Башкирский государственный университет»
Республика Башкортостан, г. Стерлитамак

ПОЗИТИВНОЕ И НЕГАТИВНОЕ ВЛИЯНИЕ СЕТИ ИНТЕРНЕТ НА ЖИЗНЕННЫЕ ЦЕННОСТИ СОВРЕМЕННОЙ МОЛОДЕЖИ

В настоящее время самыми активными пользователями сети Интернет являются молодые люди и девушки, для которых наиболее привлекательными оказались всевозможные социальные сети, онлайн-дневники, чаты, компьютерные игры, поисковые системы и др.

Интернет обладает массой достоинств, которые облегчают повседневную жизнь современного человека. Благодаря научно-техническому прогрессу ежедневное общение и обмен информацией стали происходить быстрее и удобнее.

Всем известно, что Интернет сближает общество на глобальном уровне: его используют для создания и развития бизнеса, для импорта и экспорта товаров, для отдыха и релаксации, поиска данных и любой информации, то есть для мировой торговли и коммуникации.

Систематизируем плюсы Интернет-пространства: 1) электронная почта; 2) доступ к информации; 3) покупки; 4) онлайн-общение; 5) сообщества; 6) бизнес; 7) сферы услуг.

Интернет делают притягательным следующие свойства:

1) Возможность анонимного общения, т.е. люди, могут общаться друг с другом без имени, пользуясь условным «логином», присвоенным при регистрации.

2) Возможность интерактивной реализации представлений, фантазий, невозможных в обычном мире (в том числе создание новых образов «Я» в ролевых играх, чатах и т.д.).

3) Возможность поиска нового собеседника, удовлетворяющего практически любым качествам (заметим, что нет необходимости удерживать внимание одного собеседника – в любой момент можно найти нового).

Несмотря на безусловную пользу и удобство Интернета, недостатки здесь тоже имеются и немалые. Попадая в виртуальный мир, молодежь лихорадочно «блуждает» по сети, зачастую забывая о ежедневных делах, учебе и работе, о взятых на себя обязательствах, полностью «растворяясь» в манящих и красочных сайтах. В подобных случаях речь идет об Интернет-зависимости или так называемой Интернет-аддикции.

Интернет-аддикция – это непреодолимое желание подключиться к Интернету в режиме офлайн и неспособность завершить сеанс, находясь в режиме онлайн.

По мнению психолога М. И. Дрепы, существуют несколько видов зависимости от Всемирной паутины:

1. Навязчивый веб-серфинг (информационная перегрузка) – бесконечные путешествия по Всемирной паутине, поиск информации.

2. Пристрастие к виртуальному общению и виртуальным знакомствам – большие объёмы переписки, постоянное участие в чатах, веб-форумах, избыток знакомых и друзей в сети.

3. Игровая зависимость – навязчивое увлечение компьютерными играми по сети.

4. Навязчивая финансовая потребность – игра по сети в азартные игры, ненужные покупки в Интернет-магазинах или постоянные участия в Интернет-аукционах.

При такой зависимости человек перестает искать свою реальную жизненную дорогу, откладывая в «долгий ящик» дела, затормаживая тем самым социальное и личностное развитие.

На физиологическом уровне появляется вялость, сонливость, раздражительность, тревожность, проявляется снижение работоспособности, ухудшение памяти и внимания. Свободный доступ в Интернет отбивает желание развивать взаимодействие и строить отношения с обществом на реальном, не виртуальном уровне.

Это особенно заметно среди подростков и молодых людей юношеского возраста. Последствиями продолжительного онлайн-существования становятся проблемы в обучении, снижение умственной активности, частые и беспричинные смены настроения, неадекватная реакция на критику, эмоциональное отчуждение, нарастающая оппозиционность и негативное отношение к окружающим, требующим выключить компьютер, отказ от других интересов и хобби, приступы страха, агрессии, тревоги, появление фобий, изворотливость, лживость, замкнутость, ранее не характерные личности.

В связи с поставленными выше проблемами мы провели анонимное анкетирование влияния Интернет-пространства на жизненные ценности и цели современной молодежи, в котором приняли участие студенты колледжа СФ БашГУ. Для респондентов (всего участвовало 68 человек) была разработана анонимная анкета. В ходе анализа результатов анкетирования было выявлено, что все студенты, участвовавшие в анкетировании (100 %), каждую свободную секунду посвящают общению в сети, поиску информации или онлайн-играм. На первый вопрос анкеты «Сколько времени вы проводите в Интернете?» 54 % опрашиваемых ответили, что уделяют этому более трех часов в день и только 38 % опрашиваемых осознают, что уделяют слишком много времени веб-серфингу, бесполезно теряя драгоценное время, что является психологической зависимостью от виртуального пространства.

Следовательно, Интернет (как социальные сети и информационный источник) становится неотъемлемой частью жизни и жизненной ценностью для современных молодых людей.

В ходе анализа ответов респондентов установлено, что в социальных сетях ежедневно проводят огромное количество времени 50 % опрашиваемых, в основном для обмена информацией на вербальном и мультимедийном уровнях, что удобно и дает возможность общаться на значительном расстоянии друг от друга, не выходя из дома.

Однако 33 % отвечающих подчеркнули, что живое общение, стало отходить на второй план, в некоторых случаях Интернет заменяет им реальность, что зачастую, выйдя для виртуального общения в социальные сети, они отказываются от прогулок, встреч, непосредственного взаимодействия с близкими.

Отсюда следует вывод, что основная опасность глобальной сети Интернет в иллюзорности воспринимаемой и получаемой информации – личность на самом деле находится в одиночестве перед электронным устройством, а у нее создается иллюзия полноценного общения.

По результатам анкетирования 37 % обучающихся постоянно обращаются к поисковым Интернет-ресурсам, электронным библиотекам и архивам. Чтобы расслабиться и отдохнуть – 17 % респондентов используют игровые сайты. Опрашиваемые студенты признались, что игры в сети Интернет стали потребностью, что часто они не способны своевременно завершить сеанс, возникает непреодолимая тяга изучить все уровни и стратегии, предлагаемые разработчиком игры. Подобные сайты затягивают молодого человека в новую неизведанную реальность, что постепенно приводит к печальным последствиям: конфликты с близкими, неряшливость, не успешность в учебе, разрушение круга общения, неудовлетворение реальной жизнью, отсутствие реальных жизненных целей.

Анализируя данные, обнаружено противоречие в ответах испытуемых, так более половины молодых людей и девушек диагностировали у себя наличие Интернет-зависимости, как от информационного источника. В тоже время 40 % респондентов не осознают или не хотят признавать негативного воздействия виртуального пространства глобальной сети на свою психику, хотя ежедневно многократно выходят в Интернет на длительное время через личные мобильные гаджеты и ПК.

Анализ данных результатов анкетирования выявил следующие фактические данные: половина опрошенных честно признались, что онлайн-общение стало частью жизни, и отмечают тенденцию к замене живого общения виртуальным, а 23 % опрошенных не представляют своего существования без Интернета.

У 33 % юношей и девушек возникает ежедневная потребность в использовании Интернета, связанная с учебой или работой, с поиском информации, проблема лишь в ее корректности и достоверности. 34 % – периодически пользуются просторами всемирной паутины, 26 % опрошенных признались, что развлекательные и коммуникативные ресурсы сети отвлекают от важных дел, а 10 % респондентов открыто заявили, что страдают от веб-аддикции.

Порадовало то, что 40 % студентов утверждают, что предпочитают активную, творческую и познавательную деятельность стационарному пребыванию перед монитором.

Таким образом, Интернет оказывает значительное влияние на ценностные ориентиры молодежи, он плотно вошел в обиход современного человека, грань между виртуальностью и реальностью стала очень тонкой. Недостаточно социализированные и слабые характером личности попадают под «волны» веб-пространства, полностью погружаясь в разнообразные сайты, социальные сети, чаты, форумы, онлайн-игры. Подобный «сёрфинг» приводит к негативным последствиям, влияя на ценностные ориентации подрастающего поколения: для молодого человека приоритетными становятся личные интересы, параллельно формируется безразличное отношение к обществу, социальным нормам и базовым общечеловеческим ценностям, таким как позитивное межличностное общение, сотрудничество, взаимопомощь. Постепенно обесценивается живое полноценное общение, реальный коммуникативный акт с его непосредственными эмоциями заменяется бесчувственными сухими сообщениями,

чтение книг – сомнительной информацией поисковых сайтов, психологическое здоровье – зависимостью от IT-технологий и виртуального информационного пространства в гаджетах и ПК.

В связи с вышесказанным, необходима четкая позиция со стороны государства как в отношении контроля над пространством социальных сетей в частности, так и Интернета в целом. Важно оптимально использовать их потенциал для воспитания такого молодого поколения, которое могло бы достойно встретить вызов будущего.

Список литературы

1. Дрепа М. И., Шиянов Е. Н. Интернет-зависимость и ее профилактика у студентов: учебно-методическое пособие. – Ставрополь: Графа, 2009. – 348 с.

Торгашова А. Э.
Научный руководитель – учитель истории и обществознания
Строчко Т. Н.
МБОУ «СОШ № 24 с углубленным изучением иностранного языка»
Республика Башкортостан, г. Салават

ВЛИЯНИЕ ОБЩЕНИЯ В СОЦИАЛЬНЫХ СЕТЯХ НА ГРАМОТНОСТЬ ПОДРАСТАЮЩЕГО ПОКОЛЕНИЯ

В современном мире существует множество способов виртуального общения: социальные сети, мессенджеры, программы видеосвязи и многое другое. Все это не может не оказывать какого-либо влияния на неокрепшие умы детей. Подростки все чаще пользуются сетью Интернет, при этом большую часть времени занимает именно общение. Сеть давно уже завоевала прочные позиции не только в среде профессиональной деятельности, но и стала одним из любимейших источников развлечений. Интернет – это общение с миром посредством телефона или компьютера, то есть при помощи письменного языка, а значит, всемирная сеть и грамотность тесно взаимосвязаны. В последние годы наиболее острой стала проблема снижения грамотности подростков. Чаще всего это связывают именно с виртуальным общением. **Актуальность исследования** связана, с одной стороны, с возрастающей популярностью Интернет, как способа коммуникации, особенно среди подростков, с другой стороны, с понижающейся грамотностью письменной речи у значительной части населения. **Проблемой нашего исследования** является влияние Интернета на грамотность и образованность подрастающего поколения.

В процессе исследования мы поставили перед собой **гипотезу**: общение в Интернете, включающее в себя отсутствие знаков препинания, деформацию слов и несоблюдение правил орфографии, пагубно влияет на общую грамотность подрастающего поколения.

Цель: исследовать влияние Интернета и социальных сетей на практическую грамотность подростков.

Задачи:

- изучить информацию об особенностях и формах виртуального общения подростков через Интернет;
- изучить часто употребляемые сленговые выражения и сокращения слов и выявить особенности влияния Интернет-общения на русский язык;
- исследовать мнение учащихся по этому вопросу посредством проведения опроса учащихся 9–11 классов.

На фоне всеобщей безграмотности грамотный школьник или студент сегодня – исключительная редкость, нарушение общей закономерности. Ситуация становится похожа на 1927 год, в который Л. В. Щерба написал, что пробел в образовании, связанный со снижением грамотности подрастающего поколения, «дошел до размеров общественного бедствия», и призывал срочно «изыскивать меры для его изживания» [3, с. 56]. Делая такой вывод, Л. В. Щерба и не подозревал, что данная им характеристика будет актуальна и спустя 90 лет. Но если низкую грамотность молодежи 20-х годов XX века еще как-то можно оправдать (в 1920 году умение читать было зафиксировано всего у 41,7 % населения в возрасте от 8 лет), то сейчас неумение читать или писать – удивительно, ведь обучающиеся изучают родной язык в школе и после, используются сотни программ и методов для обучения грамотному письму и правильной речи. Из этого следует, что проблема неграмотности никак не связана с несовершенствами образовательной системы.

Интернет – это особая коммуникативная среда, диктующая не только свои условия общения, но и правила речевого поведения. С начала активного использования Сети возникла новая форма языковой коммуникации – письменная разговорная речь. Она неотредактированная, спонтанная, часто зависит от ситуативности процесса говорения. Немаловажную роль играет и непринужденность общения. Войдя в сетевую сферу употребления, русский язык вынужден видоизменяться и приспосабливаться. К примеру, в Интернете покажутся неуместными книжно-письменные стили общения. Письменная речь меняется и приобретает черты разговорного стиля.

Не все простои с письмом. Механическая память руки у многих школьников и студентов не развита, так как оснащенные клавиатурой компьютер или телефон не предполагают написания слова от руки. У таких детей не могут быть сформированы, как говорит М. А. Кронгауз, «автоматизированные навыки зрительного восприятия правильного образа слова». При написании человек видит воспроизведенное слово целиком, а при наборе оно распадается на составные части – отдельные буквы. Печатающий не стремится перепроверить созданное высказывание, откорректировать его – он хочет отвечать быстро, особенно в чатах, чтобы не потерять нить разговора.

Так же на грамотность молодежи влияет и заимствованность слов из других языков. «Не люблю, когда я не понимаю отдельных слов в тексте или в чьей-то речи. Даже если я понимаю, что это слово из английского языка и могу вспомнить, что оно там значит, меня это раздражает. Позавчера я споткнулся на стритрейсерах, вчера – на трендсеттерах, сегодня – на дауншифтерах, и я точно знаю, что завтра будет только хуже. К заимствованиям быстро привыкаешь, и уже сейчас трудно представить себе русский язык без слова компьютер или даже без слова пиар» [2, с. 12].

Есть и другая, не менее важная причина снижения грамотности, о которой говорил еще Л. В. Щерба, – нелюбовь к чтению, неумение читать. «Совершенно очевид-

но, что дети, которые должны овладеть литературным языком, должны читать наших классиков… и читать их в большом количестве» [3, с. 62]. Сейчас подростки считают, что чтение совершенно необязательно, ведь всю нужную информацию они могут легко найти в Интернете за несколько кликов.

Подростки не просто пользуются Интернетом – они живут им и живут в нем. Просмотреть обновления статусов друзей в соцсети для них так же естественно, как для их родителей вынуть из кармана телефон, чтобы посмотреть, который час. Для понимания друг друга им не нужно быть грамотными, достаточно лишь улавливать суть сообщений собеседника. «Грамотность современной молодежи по сравнению с теми учениками, которые учились 5, 10, 15 лет назад, существенно отличается. Наши дети мало читают (некоторые не читают совсем). Поэтому у них не развита зрительная память. Они пишут так, как слышат. В современном Интернет-общении активно высказывается мысль о том, что при письменном общении можно не соблюдать орфографические нормы, так как это совсем не мешает взаимопониманию» [1].

Общение в социальных сетях способствует неграмотному и бездумному письму, так как предполагает анонимность пользователя, частичную или полную, дающую свободу высказываний и поступков, ведь риск разоблачения окружающими минимален. Вследствие этого в сети проявляется особенность общения – раскрепощенность, обилие ненормативной лексики и некоторая безответственность участников общения.

Чтобы узнать мнение учеников по этой проблеме, мы провели опрос среди учеников 10–11 классов. Благодаря этому было выяснено, что более 60 % опрошенных предпочитают виртуальное общение реальному; так же все участники опроса более половины времени в Интернете проводят именно в социальных сетях, то есть общаясь. На вопрос «Замечаете ли вы, что ваша грамотность страдает от такого общения?» большинство ответили, что не уделяют этому должного внимания, но думают, что отрицательное влияние присутствует.

Проанализировав весь материал, мы пришли к выводу, что есть несколько **путей решения этих проблем**:

1. Во многих гаджетах есть функция «Родительский контроль», которая позволяет родителям блокировать нежелательные сайты или же контролировать время пребывания ребенка в сети. Воспользовавшись ей, родители могут быть спокойны – их ребенок будет менее «затянут» в виртуальное общение.

2. Большинство подростков, вопреки мнению старшего поколения, являются сформировавшимися личностями. Прямой контакт с ними и обычные разговоры помогут ребенку осознать проблему и предотвратить ее.

3. Не стоит забывать, что Интернет – это источник безграничных возможностей, то есть он может помочь в борьбе с тотальной неграмотностью. Стоит всего лишь направить его в нужное русло.

4. Сделать чтение для подростков не обязанностью, а увлечением. Нужно показать, что литература не ограничивается учебниками и школьной программой.

5. Подавать пример своим детям. У кого же еще будут они учиться, если не у своих родителей?

Список литературы

1. Вишневская Н. «Городские профессии»: Учителя поражены вопиющей безграмотностью современной молодежи [Электронный ресурс] / Н. Вишневская. – Москва, 2014. URL: http://actualitati.md/ru/obshchestvo /gorodskie-professii-uchitelya-porazheny-vopiyushchey-bezgramotnostyu-sovremennoy (дата обращения: 29.01.2017).
2. Кронгауз М. А. Русский язык на грани нервного срыва. – М.: Языки славянской культуры, 2009.
3. Щерба Л. В. Безграмотность и ее причины / ред. М. И. Матусевич; Акад. наук СССР, Отд-ние лит. и яз. – М.: Учпедгиз, 1957.

Торосян М. Д.
Научный руководитель – преподаватель математики и информатики
Артемьев А. В.
Колледж Стерлитамакского филиала
ФГБОУ ВО «Башкирский государственный университет»
Республика Башкортостан, г. Стерлитамак

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ЗАЩИТЫ ИНФОРМАЦИИ В РОССИИ

Отличительной особенностью современности является переход от индустриального общества к информационному, в котором главным ресурсом становится информация.

Проникая во все сферы деятельности общества и государства, информация приобретает конкретные политические, материальные и стоимостные выражения. С учетом усиления роли информации на современном этапе, правовое регулирование общественных отношений, возникающих в информационной сфере, является приоритетным направлением процесса нормотворчества в Российской Федерации (РФ), целью которого является обеспечение информационной безопасности государства [1].

С начала 1990-х годов был дан старт объединению персональных компьютеров в локальные и международные сети, что в дальнейшем привело к созданию глобальной информационной сети Интернет.

Привычно относимое к будущему информационное общество представляет собой реальность сегодняшнего дня. Уже сейчас в наиболее экономически развитых государствах более половины рабочих мест приходится на сферу производства и обработки информации. В условиях информационного общества ключевую роль играют телекоммуникационные сети как среда для сбора и обмена информацией в локальных, общегосударственных и международных масштабах, где протекают процессы лавинообразного распространения общественных отношений по поводу использования глобальной сети Интернет.

Развитие коммуникационных технологий и широкое распространение сети Интернет в России повлекли за собой множество правовых проблем.

Являясь по сути глобальной, децентрализованной информационной средой, имеющей коммуникационную основу, глобальная компьютерная сеть Интернет представляет собой идеальный инструмент ведения экономической, и в том числе предпринимательской, деятельности с использованием новых информационных технологий. При этом в качестве несущей конструкции электронного сегмента мировой экономики рынков (мирового хозяйства) выступает возможность переноса основных элементов производственно-бытовой цепочки большинства хозяйственных процессов (т.е. развития, как отдельных производств, отраслей экономики, так и регулирующих процессов в рамках всей экономики страны, группы стран и экономик рынков целых регионов) в электронную экономическую и юридическую среду, функционирующую в режиме реального времени (on-line). Сдерживающим фактором развития данного процесса является сложность регулирования вопросов правового, таможенного, налогового и иного характера в отношении таких сделок, а также вопросов информационной безопасности и защиты прав на интеллектуальную собственность».

Термин «защита информации» подразумевает деятельность, направленную на обеспечение защищённого состояния объекта.

В соответствии с действующим уголовным законодательством Российской Федерации под преступлениями в сфере компьютерной информации понимаются совершаемые в сфере информационных процессов и посягающие на информационную безопасность деяния, предметом которых являются информация и компьютерные средства.

Данная группа посягательств являются институтом особенной части уголовного законодательства, ответственность за их совершение предусмотрена гл. 28 УК РФ [2].

По УК РФ преступлениями в сфере компьютерной информации являются:

- неправомерный доступ к компьютерной информации (ст. 272 УК РФ);
- создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ);
- нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ).

В России борьбой с преступлениями в сфере информационных технологий занимается Управление «К» МВД РФ и отделы «К» региональных управлений внутренних дел, входящие в состав Бюро специальных технических мероприятий МВД РФ.

Список литературы

1. http://www.bezpeka.com/ru/lib/spec/law/state-regulation-of-information-security-rf.html.

2. http://www.consultant.ru/document/cons_doc_LAW_10699/4398865e2a04f4d3cd99e389c6c5d62e684676f1.

Усманов И. С.
Научный руководитель – к.п.н., преподаватель математики и информатики
Трошкина Е. Ю.
Колледж Стерлитамакского филиала
ФГБОУ ВО «Башкирский государственный университет»
Республика Башкортостан, г. Стерлитамак

ЦЕННОСТНЫЕ ОРИЕНТАЦИИ СОВРЕМЕННОЙ МОЛОДЕЖИ

Современное общество находится в динамичном процессе развития, который затрагивает все сферы существования человека. Каждое общество связывает свое будущее с подрастающими поколениями, молодежью. И от того, насколько эти поколения усвоят духовные, нравственные и культурные традиции своего государства, народа и общества, таким и их будущее. Актуальность определятся наличием противостояния между современными социальными условиями формирования ценностей и сложившейся традицией социально-одобряемых норм и правил. Изучение ценностных ориентаций молодежи позволяет не только определить духовные источники развития общества, удерживающие его от саморазрушения, но и выявить, идет ли оно в направлении социокультурной модернизации или трансляции традиционных для России ценностей.

В современных научных представлениях под ценностью понимаются идеально-эталонные побуждения, цели и нормы деятельности человека, в соответствии с которыми индивид оценивает и выражает субъективное отношение, а также практически преобразует себя и мир. Если систематизировать все эти дефиниции и сформулировать определение ценности, то под ценностью выступает значимый для субъекта предмет (материальный или идеальный), способный удовлетворить его потребности и интересы. По мнению Бойкова В. Э. [1], ценности молодежи – общие представления, разделяемые общей частью молодежи, относительно того, что является желательным, правильным и полезным.

Наиболее простая классификация ценностей выделяет две основные группы ценностей: материальные и духовные.

Первую составляет совокупность выдающихся произведений интеллектуального, художественного, религиозного творчества: произведения живописи, литературы, памятники архитектуры, ремесленные изделия и т. д.

Вторая включает социальный опыт общества, «наиболее оправдавшие себя и показавшие наибольшую социальную эффективность принципы осуществления жизнедеятельности: нравы, обычаи, стереотипы поведения и сознания, образцы, оценки, образы, мнения, интерпретации и т. п., то есть принципиальные нормы поведения и суждения, которые ведут к повышению социальной интеграции сообщества, к росту взаимопонимания между людьми…».

На наш взгляд, молодежь и ее ценностные ориентиры являются большой, сложной и актуальной проблемой, которой в социологической литературе посвящено много работ. Можно сделать вывод о том, что исследования в этой области социоло-

гии необходимы для разрешения того кризиса, который переживает сегодня Россия. А связь таких аспектов проблем молодежи, как молодежная субкультура и молодежная агрессивность очевидна. Только тщательные и систематические исследования в области развития социальной работы с молодежью могут помочь понять причины происходящего в нашем обществе конфликта поколений. Необходимо понять суть молодежных исканий, отрешиться от безусловного осуждения того, что несет с собой молодежная культура, дифференцированно подходить к явлениям жизни современной молодежи. Также необходимо понять, что молодому человеку нужно определить границы своих реальных возможностей, узнать, на что он способен, утвердиться в обществе.

В молодежной среде появляются новые тенденции в понимании культуры, культурного человека и его места в будущей социальной среде. В массовом сознании восприятие молодежной субкультуры часто имеет негативный характер. На этом фоне молодежная культура со своими специфическими идеалами, модой, языком, искусством все чаще ложно оценивается как контркультура. Тем не менее, молодежь признает объективное существование историко-культурных ценностей, национальных традиций.

Методы воздействия на социализацию молодого поколения различны. Большую роль на формирование систем ценностных ориентаций молодежи оказывают изменение социального устройства, законодательной базы, видов социальной защиты, способов хозяйствования, экономической ситуации. Однако, вне зависимости от наличия или отсутствия ресурсных возможностей, участвовать в процессе формирования систем позитивных ценностных ориентаций молодёжи должны все субъекты молодёжной политики: государство, религиозные конфессии, политические партии, общественные организаций и корпорации.

Процесс формирования систем ценностных ориентаций современной российской молодёжи представляет собой сложный, комплексный, многоаспектный процесс, требующий разработки единой стратегии и объединения усилий общественных и государственных составляющих молодёжной политики. Для эффективного функционирования институтов социализации и воспитания молодёжи, как инструментов и факторов формирования ценностных ориентаций современной российской молодёжи требуется соблюдение таких условий, как четкое определение целей, функций деятельности каждого института; скоординированность действий всех институтов; оптимизация деятельности существующих или появление новых институтов.

Активно взаимодействуя между собой, субъекты молодёжной политики должны достигнуть единства духовных и идеологических установок, создать единое воспитательно-педагогическое пространство; выработать единый алгоритм действий по преодолению кризиса институтов социализации; обеспечить воспитание самостоятельной, идейной, одухотворённой, ответственной молодёжи и формирование у неё системы позитивных традиционных ценностных ориентаций.

Особая роль в этом процессе принадлежит государству. Ведь государство обладает наибольшими ресурсами и возможностями для осуществления целостной молодёжной политики, координируя свою деятельность с её общественной составляющей.

Список литературы

1. Бойков В. Э. Ценности и ориентиры общественного сознания россиян. СОЦИС. – 2004. – № 7.

Фаизова Д. Р.
Научный руководитель – преподаватель юридических дисциплин
Голубничий А. С.
Колледж Стерлитамакского филиала
ФГБОУ ВО «Башкирский государственный университет»
Республика Башкортостан, г. Стерлитамак

ПРОБЛЕМА НОРМАТИВНО-ПРАВОВОГО РЕГУЛИРОВАНИЯ «DARKNET»: РОССИЙСКАЯ ДЕЙСТВИТЕЛЬНОСТЬ И ЗАРУБЕЖНЫЙ ОПЫТ

Разговоры о том, что цифровые медиа меняют наш мир на ходу, давно стали общим местом. Мы не замечаем, но Интернет занимает в нашей повседневной жизни всё больше значимого места. Сами того не замечая, мы пользуемся Интернет-ресурсами «каждый божий день» и не понимаем какую угрозу он в себе утаил и подвергаем свою Интернет жизнь различного рода опасностям. Стоит задуматься всегда ли Интернет несет только пользу, ведь все мы прекрасно понимаем, что существуют и некая «темная сеть» Интернета, в которой имеет место быть и терроризм, и торговля различными видами оружия, и детская порнография, которая имеет свое распространение в неком Интернет-ресурсе под названием DarkNet о котором будет сказано чуть позже. Невольно задаешься вопросом: Ведётся ли борьба с данным видом угрозы?

Мы привыкли воспринимать Интернет довольно однобоко. Большинство пользователей уверены, что это только то, что мы видим в нашем браузере. Чтобы понять, что представляет из себя эта скрытая «темная сеть», называемая DarkNet необходимо понять, на чем акцентируется информация, содержащаяся в данном Интернет-ресурсе. Итак, DarkNet это более высокий по степени анонимности сегмент Интернета, информация в котором попадает лишь человеку, запрашиваемому данную информацию. Эта сеть, к которой невозможно подключиться через обычный браузер. В нём сконцентрированы сообщества, занимающиеся незаконной деятельностью, детской порнографией, в том числе торговлей запрещенными товарами, такими как оружие, банковские карты, наркотики, подделанные документы, паспорта, водительские удостоверения и другое. В настоящее время в DarkNet можно найти всё, что угодно, например, социальные сети, много ресурсов с украинской тематикой, а именно запрещенные политические партии, запрещенная информация, в которую входит изготовление взрывчатых устройств, наркотических средств и т.п. Так же на данных Интернет серверах имеются украденные базы аккаунтов, данные банковских карт, имеет место и покупка поддельных документов. Многие люди выбирают эту сеть ради сохранения приватности и свободы слова.

Для осуществления деятельности на данных сайтах существует некий браузер под названием Tor, позволяющий анонимное сетевое соединение, защищенное от прослушивания, и просто запароленные сайты, недоступные широкой публике, и неиндексируемые поисками базы данных, и контент, намеренно спрятанный от поисковых машин. Также Tor позволяет Вам посещать и даже создавать недоступные обычным пользователям сайты с собственным доменным именем. На сегодняшний день Tor является одним из самых популярных даркнетов.

Если существует подобная угроза, должна существовать и защита от подобных Интернет-ресурсов. Многих интересует вопрос, как власти борются с данными Интернет сетями, и существует ли данная защита вообще.

К сожалению, на данный момент в России отсутствует законодательная база по отслеживанию теневых ресурсов, что неблагоприятно сказывается на деятельности многих сетей Интернета и не только. Но стоит отметить, что борьба с угрозами, возникающими на «просторах Интернета» всё же находится на стадии разработки. Не стоит упускать и тот момент, что правоохранительные органы ведут работу над выявлением и привлечением к ответственности злоумышленников, скрывающих свою активность при помощи Tor и иных инструментов для сохранения анонимности. Так, например, министр связи и массовых коммуникаций Российской Федерации Николай Никифоров выразил обеспокоенность фактом существования даркнета и активностью в нем различных криминальных элементов. Никифоров не исключил в перспективе возможности разработки и поэтапного внедрения в жизнь законодательной базы для регулирования использования браузеров.

В отличие от РФ существует ряд стран, которые занимаются защитой своих граждан от угроз, исходящих от неблагоприятных интернет ресурсов. Одной из таких стран является Китай. Интернет в Китае появился в 1994 году. В 1998 г. правительство осознало, что пришло время подумать о защите народных масс от вредоносной информации и началась разработка системы «Золотой Щит», которая была запущена в 2003 году. Прежде всего, его основной целью является цензура и контроль всей онлайн-активности как в Китае, так и за его пределами от детской порнографии и политической дезинформации. Согласно официальному законодательству для этого проекта, веб-сайты, базирующиеся на территории Китая, не могут ссылаться и публиковать новости, взятые из зарубежных новостных сайтов, или СМИ без специального одобрения. Существует список медиа-сайтов, которые имеют разрешение публиковать новости в Интернете. Все другие веб-сайты могут предоставлять только ту информацию, которая уже обнародована уполномоченным СМИ. Они также должны получить одобрение со стороны информационного агентства Государственного Совета и несут ответственность за законность транслирования информации. Каждый Интернет-провайдер информационных услуг «должен сохранять копии записей в течение 60 дней» и быть готовым предоставить эту информацию для органов государственной власти по первому требованию. Провайдеры, также, обязаны ограничивать информацию, которую они публикуют. Несоблюдение любого из вышеупомянутых требований приводит к заблокированию веб-сайта.

В заключение хотелось бы сказать следующее, что независимо, в какой стране распространяется та или иная «темная сеть» будь то Россия или Китай необходимо знать к чему может привести использование данной сети в деле и уметь защитить своих граждан от вреда, наносящегося данными Интернет ссылками.

Список литературы

1. Джейми Бартлетт «Даркнет: цифровое подполье» // URL: http://bookz.ru/authors/djeimi-bartlett/podpol_n_934/1-podpol_n_934.html(дата обращения 23.02.2017).

2. Великий китайский золотой щит // URL: https://habrahabr.ru/company/websitepulse/blog/136072/ (дата обращения 23.02.2017).

Хайретдинова Л. И.
Научный руководитель – преподаватель математики и информатики
Лысенко Д. В.
Колледж Стерлитамакского филиала
ФГБОУ ВО «Башкирский государственный университет»
Республика Башкортостан, г. Стерлитамак

ИНТЕРНЕТ-ЗАВИСИМОСТЬ МОЛОДЕЖИ ОТ СОЦИАЛЬНЫХ СЕТЕЙ КАК ПРОБЛЕМА СОВРЕМЕННОСТИ

Актуальность работы состоит в следующем. Широкое внедрение информационных технологий в жизнь современного человека имеет как позитивные, так и негативные последствия. Отрицательными последствиями длительного использования информационных технологий являются сужение круга интересов, уход от реальности в виртуальный мир и развитие зависимости. Открывшиеся Интернет-возможности поглотили большую часть молодежи. С одной стороны, увеличение количества пользователей Интернета студенческого возраста, разработка новых скоростных программ общения и виртуального взаимодействия, а с другой – отсутствие комплексных мер, включающих психологическую профилактику, привело к росту Интернет-зависимости.

Цель – исследование причины зависимости молодежи от социальных сетей и разработать рекомендации по профилактике зависимости молодежи от социальных сетей.

Задачи:

1. Провести исследование социального общества для выявления причин зависимости молодежи.
2. Выявить влияние Интернет-зависимости на уровень здоровья молодежи.
3. Разработать рекомендации по профилактике зависимости молодежи от социальных сетей.

В современном обществе достаточно популярен термин «всемирная паутина», хотя 15–20 лет назад для большей части жителей нашей страны он был незнаком. Ситуация поменялась кардинально с развитием технического прогресса, повышением доступности использования Интернета, с каждым годом растет число пользователей и как следствие увеличивается число людей, проводящих много времени в виртуальном пространстве. Замещение реальной жизни благодаря компьютерным технологиям отдаляет человека от непосредственного общения, в котором каждый участник может развиваться, получать информацию, сопровождаемую эмоциональным контекстом. Отсутствие полной обратной связи в общении ведет к искаженному восприятию собеседника и реальности.

Основная функция социальных сетей – обеспечивать поддержание связи между людьми, даже когда они находятся далеко друг от друга. Каждый человек может посредством социальных сетей легко общаться с друзьями и коллегами, а также произвести поиск людей, связь с которыми была прервана, и обзавестись новыми прият-

ными знакомствами. На сегодняшний день нередки случаи, когда в результате знакомства молодых парней и девушек образуются новые семьи. Просмотр фотографий, видеофильмов, прослушивание аудио-музыки. Если у вас появились новые фотографии, которые вы очень хотите показать своим друзьям, если вы хотите легко найти фильм с целью его просмотра или послушать любимые аудио хиты без длительного их поиска по другим музыкальным сайтам – социальные сети вам в помощь.

Самым интересным было выяснить общую зависимость молодежи от социальных сетей. Это было сделано с помощью преобразования ответов в анкете в процентное соотношение зависимости. Всего было опрошено 50 человек, в анкете содержалось 17 вопросов с вариантами ответов, а также возможность заполнения строки – свой вариант.

Средняя зависимость в сумме по всем анкетам равна 46 %. Это значит, что люди практически на 50 % зависят от социальных сетей. Термин «зависимость от социальных сетей» психологи выделили недавно. До этого выделялся термин «зависимость от Интернета». Социальные сети набирают всё большую популярность. Чаще всего, ими пользуются подростки и молодые люди до 30 лет [2]. Так как наше исследование было среди студентов, то в основном в нем участвовали лица от 16 до 20 лет. Все опрошенные на вопрос «есть ли вы в социальной сети» ответили положительно, каждый зарегистрирован «Вконтакте» – 100 %, а также встречаются «мой мир» – 50 %, «одноклассники» – 20 %, «Facebook» и «Instagram» по 10 % от числа всех опрошенных. Далее вопросы исходили из темы статьи, наиболее интересные результаты: «Сколько раз в неделю вы заходите на свою страницу в социальных сетях?» – 95 % отвечают, что каждый день посещают страничку, 5 % два – три раза в неделю. При этом в день по два – три часа проводят 32 %, четыре – шесть часов или весь день без учета сна по 20 % отпрошенных, и 18 % час или два часа в день. Время проведения в социальной сети чаще всего приходится на день и вечер. Наиболее важные аспекты интересов в социальной сети это общение с друзьями и знакомыми людьми 95 %, а также выбирали такие варианты ответов как просмотр интересных фактов и страниц, прослушивание музыки. Доверяют полученной информации из социальных сетей 60 % опрошенных. Желание специально сфотографироваться и тут же разместить свои фото в сеть имеют 20 % опрошенных, иногда желают сфотографироваться специально для социальной сети 60 % и 20 % вообще не испытывают такого желания. Всегда интересно знать, что происходит на их социальной странице 65 % опрошенным, а остальным либо не интересно, либо иногда. Общение в социальных сетях чаще приятнее, чем в реальном мире лишь 8 % опрошенных, 80 % отмечают, что иногда общение в социальных сетях приятнее, чем в реальности, остальные 12 % никогда не заменят реальное общение социальным сетям. 72 % опрошенных утверждают, что никогда не сорились с близкими из-за проведения времени в социальных сетях, иногда возникают конфликты у 23 % опрошенных, и часто возникают ссоры у 5 %. Внимательно просмотрев результаты тестирования можно выявить что молодежь, проходившая данное исследование в общем виде не имеет серьезных проблем связанных с зависимостью от социальных сетей. Есть лишь малый процент с явными признаками зависимости, так же встречаются такие ответы, которые вообще не имеют признаков данной привычки. Под термином «привычка» подразумевается влечение субъекта к определенному чувству удовле-

творения. При этом субъекту не удается справиться с этим порывом, он чувствует навязчивое желание совершать определенное действие, которое может быть вредоносным как для самого субъекта, так и для окружающих. Все формы зависимости, как и рассматриваемый, случай Интернет-зависимости, характеризуются поиском чувства удовлетворения, в данном случае – при пользовании Интернетом. В результате увеличивается время, которое затрачивается на достижение этого чувства. При этом отсутствие Интернета может быть равносильно стрессовой ситуации. Очень интересный вопрос о конфликтах детей и их членов семьи по поводу проведения времени в Интернете. Мир стремительно меняется, и это нельзя игнорировать. Когда-то людей пугали книги, которыми молодежь увлекалась чересчур. Потом – фильмы. Потом – компьютеры. Потом – игры. Сейчас – социальные сети. В этом есть правда, а есть – веяние времени. Конечно, родителей беспокоит времяпровождение своего ребенка и на фоне недопонимая, возникают конфликты. Людям недостаточно иметь только хорошие и устойчивые отношения друг с другом. Необходим социальный интерес, определенная динамика жизни, которая приносит новые впечатления. Восприятие человека все время нацелено на некоторые изменения, новые ситуации. Поэтому слишком статичные, неизменные отношения между людьми, лишенные динамики и не сопровождающиеся теми или иными событиями, со временем иссякают. Людям становится скучно, неинтересно друг с другом, и они стремятся прервать общение – чем и объясняется «чистка» контакт-листов у пользователей социальных сетей с целью удаления неактивных пользователей с необновляемыми, статичными страничками. В то же время общение может включать в себя весьма сомнительную замену реальных событий – обсуждение других людей на основе слухов и сплетен – а в социальных сетях есть возможность создавать собственные события, подкрепляя фактаж аудиовизуальным сопровождением.

Многие молодые люди становятся заложниками виртуального имиджа. В зависимость часто попадают те, кто создал свой идеальный образ, посредством аккаунта. Таким образом, люди стараются самоутвердиться, особенно если в реальности все не так безоблачно, как на страницах их профиля. Как правило, они не стремятся встретиться в жизни, потому что боятся предстать перед людьми такими, как они есть в действительности.

Социальные сети стали в современных условиях мощными инструментом влияния на молодое поколение. Такие классические институты социализации как семья, школа, сверстники отошли на второй план. Иллюзорный, виртуальный мир становится все более притягательным для молодых людей. Он не только предоставляет возможность рассказать о своих чувствах, переживаниях, но и предоставляет возможность доступа к личной информации других людей. Погружаясь в него, они даже не задумываются о том, что есть вероятность формирования «зависимости от виртуальности». Убегая от реальных проблем в виртуальный мир, молодые люди, не осознавая это, начинают воспринимать его как часть реального.

Список литературы

1. Малыгин В. Л., Хомерики Н. С., Смирнова Е. А. Интернет-зависимое поведение // Журнал неврологии и психиатрии. – М., 2011. – С. 86–92.

2. Янг К. Диагноз – Интернет-зависимость // Мир Интернет. – 2000. – № 2. – С. 24–29.

3. Ениколопов С. Н., Ерофеева Л. В., Соковня И. Профилактика агрессивных и террористических проявлений у подростков: Метод. пособие для педагогов, школьных психологов, родителей / Под ред. Соковни И. И. – М.: Просвещение. – 2002.

4. Балонов И. М. Компьютер и подросток. – М., 2002. – С. 32–58.

Хайритдинова Л. Р.
Научный руководитель – учитель истории и обществознания
Строчко Т. Н.
МБОУ «СОШ № 24 с углубленным изучением иностранного языка»
Республика Башкортостан, г. Салават

ВЛИЯНИЕ ИНТЕРНЕТА НА ПОДРОСТКОВ В КОНТЕКСТЕ РАЗВИТИЯ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА

Современное общество можно охарактеризовать как информационное общество, главным богатством которого является информация. Объективной закономерностью развития такого общества стала интенсификация информационных процессов: возрастают скорости передачи сообщений; увеличивается объем передаваемой информации; ускоряется ее обработка. Этот процесс может оказывать негативное влияние на человека, приводя к информационным перегрузкам, что в свою очередь ослабляет способность думать, размышлять.

Данная тема особенно **актуальна** сегодня, когда речь заходит об отсутствии контроля над рынком средств массовой информации, неконтролируемой подаче информации различной аудитории, что, в конечном счете, пагубно сказывается на формировании морально-нравственных ценностей подрастающего поколения.

Целью данной работы является изучение аспектов влияния Интернета как средства массовой информации на сознание молодежи. Данная цель достигается последовательным решением следующих **задач**:

1) выявить сущность влияния Интернета на сознание человека;

2) провести исследование и интерпретировать его результаты;

3) найти пути решения данной проблемы.

Проблемой исследования является сознание молодежи, подвергающееся влиянию Интернета.

Величайшее изобретение человечества – глобальные компьютерные сети – также хранят в себе потенциальные угрозы. В книге «Как пережить технологическое изменение мозга», автор Гарри Смолл пишет: «…поскольку Интернет уменьшает способность концентрироваться и созерцать, то… мышление становится отрывочным, чтение – поверхностным. Пользователи лишь по диагонали просматривают заголовки и аннотации. А зоны мозга, отвечающие за абстрактное мышление и сопереживание, практически атрофируются».

Вхождение юных россиян в Интернет-пространство, согласно данным интервью, изменило не только источники информации, медиасреду, но и весь их образ жизни. Подростки не просто пользуются Интернетом, они живут посредством его. Это среда обитания, способ жизни при содействии информационных технологий [1, стр. 32].

Подрастающее поколение с большим опережением живет по данной модели, используя для принятия решений коммуникацию со сверстниками и взрослыми. Помимо реального общения – это Интернет-коммуникация, которая у подавляющего большинства подростков, как показали массовый опрос и интервью, на первом месте. Подростки, у которых есть техническая возможность, находятся в непрерывном Интернет-контакте с друзьями, даже на школьных переменах и уроках [2, стр. 64].

Происходит постоянное расширение информационного и жизненного пространства юных россиян. Современное Интернет-поколение можно охарактеризовать как глобальных детей, у которых неограниченные возможности получения и переработки информации, знаний. При этом благодаря открытой и всеобъемлющей информации в Интернете дети стали практически независимы от взрослых в получении интересующих их сведений и знаний. Если в 2005 г. 31,7 % респондентов отмечали, что не смогли найти интересующую их информацию, то в 2012 году – это 22 %.

Отчетливо прослеживается стремление подростков к самостоятельному выбору информационных каналов и форм получения сведений. Интернет переструктурировал информационное пространство российских подростков. В поисках информации в совокупности используется многообразный спектр коммуникационных источников и механизмов, образующих медиасреду. Если в 1998 и 2005 году на первое место вышли межличностные каналы информации (сверстники, родители, учителя), то в 2012 году со значительным опережением лидируют компьютерные источники, Интернет – 72 %. Это двукратное увеличение по сравнению с 2005 г. (30,9 %) [4, стр. 2].

Время и характер пребывания подрастающего поколения в Интернете.

Характеристикой активности подрастающего поколения является время пребывания детей и подростков в Интернете, которое значительно выше, чем у взрослых. Основной диапазон, выявленный с помощью глубинных интервью: от 1 до 5 часов ежедневно. Исследования Фонда Развития Интернет подтверждают эти данные: только пятая часть подростков проводит больше 21 часа в неделю (3 часа в день) в Интернете. Это одна группа юных пользователей Интернета. Во вторую группу входит каждый восьмой школьник, который ответил, что он «живет в Интернете». Это выражение объединяет и время, которое они там проводят, отбирая его даже от сна и питания, и личную значимость его. Есть прогноз, что время пребывания будет увеличиваться за счет новых технических средств.

Экспертный анализ позволил выявить факторы, которые определяют время пребывания в Интернете [3, стр. 3]:

1. Техническая и финансовая доступность Интернета для длительного пользования.
2. Привлекательность самого контента в Интернете, особенно в случае социальных сетей и онлайн-игр.
3. Роль Интернета как комплексного средства, позволяющего читать газеты и книги, смотреть телепередачи и кино.
4. Роль Интернета в учебной деятельности.
5. Наличие свободного времени как такового.

6. Структура свободного времени, наличие других интересов и занятий.

7. Контроль родителей.

8. Самоконтроль.

Динамичный интерфейс Интернета – это комфортное пространство для ребенка. В Интернете он чувствуют себя как рыба в воде. Он для них удобен, это и средство развлечения, и средство доступа к миру информации.

Плюсы Интернета состоят в том, что сеть предлагает образовательный и полезный опыт, правильное использование которого может улучшить их успеваемость в школе или институте. Но и здесь есть свои недостатки, такие как неточные данные, а также неподходящие для детей и подростков в области информации [4, стр. 12].

Одним из негативных эффектов глобальной компьютерной сети является широкое распространение различной информации сомнительного содержания. Существуют сайты, посвященные порнографии, пиротехнике, суициду, обсуждению действия тех или иных наркотиков. Отсюда может последовать увлечение всеми этими угрожающими их здоровью вещами.

Встреча с опасными людьми в чатах или других областях. По статистике, это самый большой риск. Подростки могут войти в такие не желательные для них компании, как радикальные политические группы, сатанинские культы.

Вовлечение в азартные игры. Даже простые игрушки наносят непоправимый вред, занимая у ребенка подавляющую часть времени, отвлекая его от занятий и спокойного отдыха, вредя психическому и физическому здоровью.

Уход детей в Интернет может быть проблемой не столько технологической, сколько психолого-педагогической и социальной [3, стр. 6].

По мнению психологов, анонимность и отсутствие запретов освобождают скрытые комплексы, стимулируют людей изменять здесь свой стиль поведения, вести себя более раскованно и даже переходить некоторые нравственные границы.

Нередко виртуальная паутина настолько обволакивает, что вырваться из нее дети и подростки уже не в силах. Для них компьютерные игры или использование Интернета превращаются в реальную жизнь, заменяя активную социальную деятельность, хобби и творчество, общение со сверстниками и даже противоположным полом.

«Интернет-зависимость» – это термин, описывающий непреодолимое желание пользоваться Интернетом. В последнее время среди специалистов также стало популярным понятие «патологическое использование компьютера», которое описывает ситуации, когда компьютер служит источником для получения информации, далеко выходящей за пределы профессиональных или учебных интересов, а также для вовлечения во взаимодействие с людьми.

Большую роль СМИ играют в развитии ребенка. Появление каждого кардинально нового источника информации вызывало споры о том, во благо он или во вред человеку [4, ст. 56].

На наш взгляд, есть несколько **путей решения данной проблемы** [5, ст. 135]:

1. Нужно научить ребенка правильно вести себя в сети.

2. Заведите несколько ежедневных традиций (например, во время приема пищи – никаких ТВ и телефонов-компьютеров за столом).

3. Как можно чаще увозите ребенка из города. Поищите интересные и безопасные способы отдыха – катамараны, горные тропинки, прогулки на лошадях, путешествия, велосипедные прогулки из города в город с ночевками в палатках, и пр.

4. Поставьте, так называемые сайты-блоки на те сайты, которые не безопасны ребенку.

Мы рассмотрели тему влияния СМИ на поведение молодежи, и теперь можно с уверенностью сказать, что воздействие средств массовой информации существует и оно достаточно существенное. Молодежь – это такая социальная группа, которая очень сильно поддается влиянию масс-медиа. Также перед нами был выдвинут важный вопрос, а именно, вопрос о характере влияния СМИ. Выяснилось, что существует как позитивное, так и негативное медиа-воздействие на молодых людей, и всё чаще сейчас говорят о негативном воздействии средств массовой информации, которое выражается в их неадекватном поведении в обществе.

Список литературы

1. Влияние средств массовой коммуникации на интересы детей. – М.: Изд-во Академии педагогических наук СССР, 1999. – С. 283.

2. Войскунский А. Е. Психологический журнал. – 2004. – Т. 25. – № 1. – С. 90.

3. Глинская М. Информатизация образования – путь к построению информационного общества. – М., 2010. – С. 159.

4. Грушин Б. А. Мнение о мире и мир мнений. – М.: Политиздат, 1967. – С. 64.

5. Компьютерная газета. – Киев, 2002. – № 18. – С. 3.

Шарипова И. Ф.
Научный руководитель – преподаватель юридических дисциплин
Талачева Э. Ф.
Колледж Стерлитамакского филиала
ФГБОУ «Башкирский государственный университет»
Республика Башкортостан, г. Стерлитамак

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Внедрение новых информационно-телекоммуникационных технологий в повседневную деятельность привело к возникновению новой области юридических отношений, связанных с обменом информацией без использования бумажного носителя. Современные технологии обмена данными создают средства, не идентичные по своим функциям традиционным средства. Поэтому подобные отношения требуют особого правового регулирования.

Еще в советское время, когда создавалась основа правового регулирования отношений по использованию информационных технологий и применению автоматизированных систем, было отмечено, что информационные системы не смогут функционировать без правового обеспечения. При этом в правовом обеспечении можно различать общую и локальные части. Общая часть охватывает нормативные акты,

касающиеся задач, функций средств электронного документооборота. Локальная часть охватывает нормативные акты, издаваемые в рамках отдельных элементов информационных систем и устанавливающие задачи и функции этих элементов, права и обязанности субъектов.

Рассмотрим нормативное обеспечение работы с электронными документами в Российской Федерации.

Согласно ст. 160 Гражданского кодекса Российской Федерации «использование при совершении сделок факсимильного воспроизведения подписи с помощью средств механического или иного копирования, электронно-цифровой подписи либо иного аналога собственноручной подписи допускается в случаях и в порядке, предусмотренных законом, иными правовыми актами или соглашением сторон» [1]. В соответствии со статьей 434 Гражданского кодекса Российской Федерации договор в письменной форме может быть заключен путем составления одного документа, подписанного сторонами, а также «путем обмена документами посредством почтовой, телеграфной, телетайпной, телефонной, электронной или иной связи, позволяющей достоверно установить, что документ исходит от стороны по договору». В ст. 847 установлено, что договором может быть предусмотрено удостоверение прав распоряжения денежными суммами, находящимися на счете, электронными средствами платежа и другими документами с использованием в них аналогов собственноручной подписи, кодов, паролей и иных средств, подтверждающих, что распоряжение дано уполномоченным на это лицом. Таким образом, Гражданский кодекс Российской Федерации делает возможным использование электронных документов, заверенных электронно-цифровой подписью, во всех случаях, когда требуется письменная форма сделки, за исключением тех, при которых установлены специальные требования к форме документа (специальная бумага, мастичная печать и т. п.). Тем не менее, приведенные положения не обеспечивают возможности широкого использования электронного документооборота в гражданском обороте.

В ст. 9, 10 и 13 Федерального закона «О бухгалтерском учете» предусмотрена возможность составления и хранения первичных и сводных (регистры бухгалтерского учета и бухгалтерская отчетность) учетных документов на машинных носителях информации [3]. Согласно п. 8 ст. 12 Федерального закона «О государственной регистрации прав на недвижимое имущество и сделок с ним» Единый государственный реестр прав на недвижимое имущество и сделок с ним (далее также Реестр) в районах (городах), где имеются возможности, ведется на магнитных носителях. Однако при несоответствии записей в Реестре на бумажном и магнитном носителях приоритет имеет запись на бумажном носителе.

Указом Президента Российской Федерации от 3 апреля 1995 г. № 334 «О мерах по соблюдению законности в области разработки производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации» [4] была запрещена «деятельность юридических и физических лиц, связанная с разработкой, производством, реализацией и эксплуатацией шифровальных средств, а также защищенных технических средств хранения, обработки и передачи информации, предоставлением услуг в области шифрования информации, без лицензий, выданных Федеральным агентством правительственной связи и информации при Президенте Российской Федерации» (п. 4). Тем же Указом государст-

венным организациям и предприятиям запрещено использование «шифровальных средств, включая криптографические средства обеспечения подлинности информации (электронная подпись) и защищенных средств хранения, обработки и передачи информации», не имеющих сертификата (п. 2). Кроме того, Центральному банку Российской Федерации предложено «принять меры» к коммерческим банкам, использующим не сертифицированные защищенные технические средства хранения, обработки и передачи информации» при обмене информации с подразделениями Центрального Банка Российской Федерации (п. 3).

В настоящее время в России действует лишь один федеральный закон, непосредственно регулирующий вопросы применения электронных документов в договорных отношениях, – Федеральный закон «Об электронной цифровой подписи», который закрепляет правовые условия для использования электронной цифровой подписи в процессах обмена электронными документами, при соблюдении которых электронная цифровая подпись признается юридически равнозначной собственноручной подписи в документе на бумажном носителе (ст. 4). При этом в указанном Законе прямо предусмотрено, что его действие не распространяется на отношения, возникающие при применении иных аналогов собственноручной подписи (п. 2 ст. 1).

Основные положения Федерального закона «Об электронной подписи» устанавливают: права и обязанности обладателя электронной цифровой подписи (ст. 11 и 12); требования к сертификату ключа подписи, который выдается удостоверяющим центром, ответственным за подтверждение подлинности электронной цифровой подписи, и состав обязательных сведений, включаемых в этот сертификат (ст. 6); порядок выдачи, хранения, приостановления действия и аннулирования сертификатов ключей подписи (ст. 7, 13 и 14); функции и правовой статус удостоверяющих центров (ст. 8, 9 и 15); общие условия использования и сертификации средств электронной цифровой подписи, применяемых для создания и подтверждения подлинности ЭЦП (ст. 5); порядок признания иностранного сертификата цифровой подписи (ст. 18) [2].

Таким образом, Федеральный закон № 63 заложил основы решения проблемы обеспечения правовых условий для использования электронной цифровой подписи в процессах обмена электронными документами.

Список литературы

1. Гражданский процессуальный кодекс Российской Федерации от 14.11.2002 г. № 138 (ред. от 31.12.2014) // Собрание законодательства Российской Федерации. – 2013. – № 46.

2. Федеральный закон от 6.04.2011 г. № 63-ФЗ «Об электронной подписи» (ред. от 23.06.2016) // Собрание законодательства Российской Федерации. – 2011. – № 15.

3. Федеральный закон от 06.12.2011 № 402-ФЗ «О бухгалтерском учете» // Собрание законодательства РФ. – 2011. – № 50.

4. Указ Президента РФ от 03.04.1995 № 334 «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации» (ред. от 25.07.2000) // Собрание законодательства Российской Федерации. – 1995. – № 15.

Научное издание

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СЕТИ ИНТЕРНЕТ: ПРОБЛЕМЫ И ПУТИ РЕШЕНИЯ

Сборник материалов

I Республиканской научно-практической конференции
школьников 9–11 классов и студентов
учреждений среднего профессионального образования
г. Стерлитамак, Республика Башкортостан, 25 февраля 2017 г.

Ответственный редактор – заведующий колледжем **Надежда Николаевна Ткачева** (Стерлитамакский филиал БашГУ)

Начальник ИИЦ *О.А. Шарипова*
Компьютерная верстка *Н.С. Усманова*

Печатается в авторской редакции.
Авторы, редакционная коллегия несут ответственность за достоверность материалов, изложенных в книге.

Подписано в набор 10.04.2017 г.
Подписано в свет 11.05.2017 г.
Бумага офсетная.
Печать оперативная.
Тираж 300 (1-й завод – 30) экз.
Заказ № /17.

Подписано в печать 24.04.2017 г.
Формат $60\times84_{1/16}$.
Гарнитура «Times».
Уч.-изд. л. 12,3.
Усл. печ. л. 12,5.

Информационно-издательский центр
Стерлитамакского филиала БашГУ:
453103, г. Стерлитамак, пр. Ленина, 49.