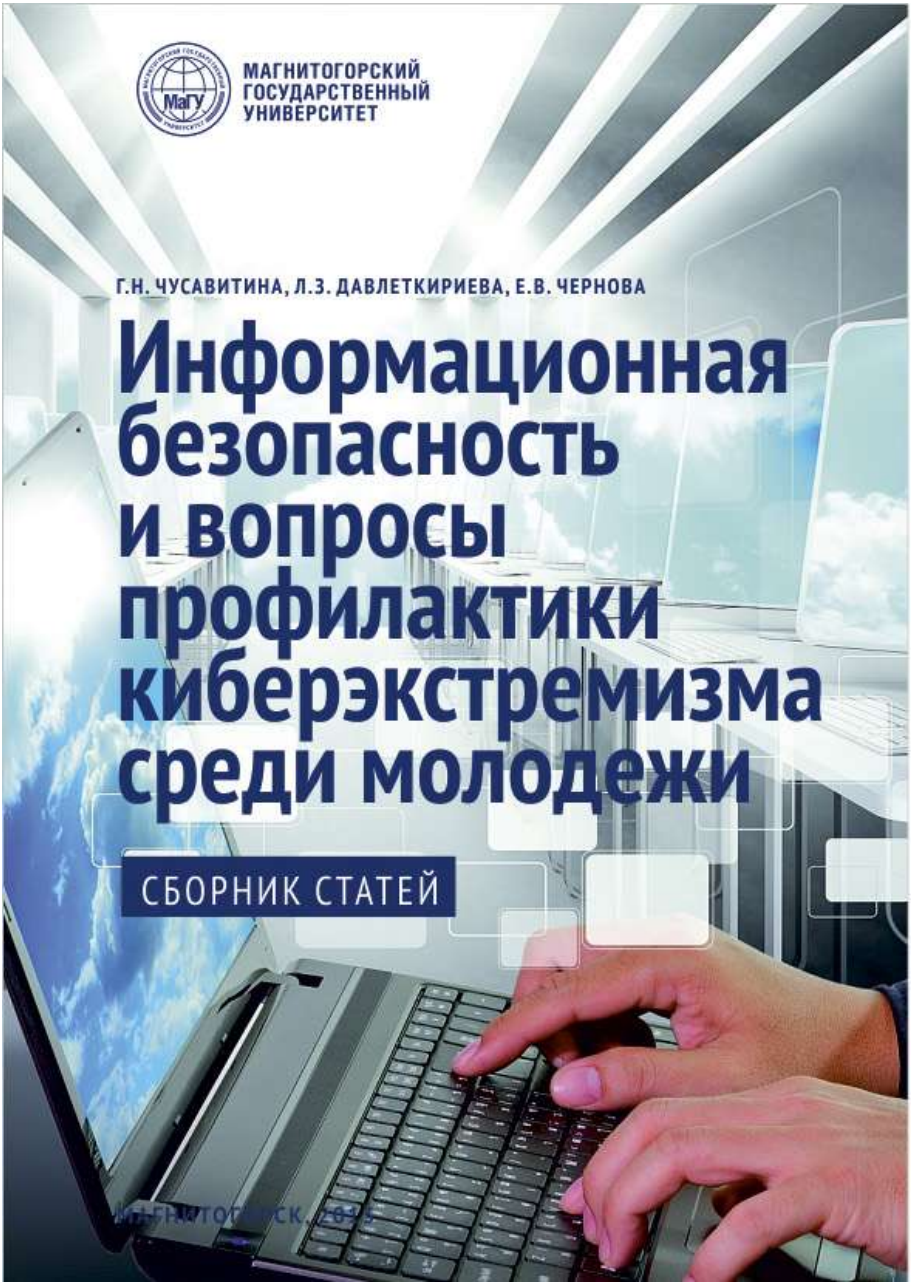

МАГНИТОГОРСКИЙ
ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ
Г.Н. ЧУСАВИТИНА, Л.З. ДАВЛЕТКИРИЕВА, Е.В. ЧЕРНОВА
Информационная безопасность и вопросы профилактики киберэкстремизма среди молодежи
СБОРНИК СТАТЕЙ

Министерство образования и науки Российской Федерации
ФГБОУ ВПО «Магнитогорский государственный университет»

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ВОПРОСЫ ПРОФИЛАКТИКИ КИБЕРЭКСТРЕМИЗМА СРЕДИ МОЛОДЕЖИ

Сборник статей

Магнитогорск
2013

ББК 3973.23
УДК 004.41
И 741

Информационная безопасность и вопросы профилактики киберэкстремизма среди молодежи (сборник статей) / под ред. Г.Н. Чусавитиной, Л.З. Давлеткириевой, Е.В. Черновой. - Магнитогорск: МаГУ, 2013. – 162 с.

ISBN 978-5-4463-0050-1

Общая редакция: **Г.Н. Чусавитина, Л.З. Давлеткириева, Е.В. Чернова**

Сборник может быть полезен научным работникам, аспирантам, преподавателям, которые интересуются проблемами подготовки научно-педагогических кадров к обеспечению информационной безопасности в ИКТ-насыщенной среде, профилактики и противодействия идеологии киберэкстремизма среди молодежи.

Издание публикуется при поддержке Российского гуманитарного научного фонда в рамках гранта № 13-06-00156 «Подготовка педагогических кадров к профилактике и противодействию идеологии киберэкстремизма среди молодежи».

ISBN 978-5-4463-0050-1

ББК 3973.23
УДК 004.41

СОДЕРЖАНИЕ

Беззубкова Ю.А., *студентка факультета информатики*
Романова М.В., *к. п. н., доц. каф. информационных технологий*

СОЦИАЛЬНО-ПСИХОЛОГИЧЕСКИЕ ПРИЧИНЫ ВОЗНИКНОВЕНИЯ КИБЕРЭКСТРЕМИЗМА

ФГБОУ ВПО «Магнитогорский государственный университет,
julia04-04@mail.ru

Аннотация

В статье описаны социальные и психологические причины, способствующие возникновению киберэкстремизма. Рассмотрены предпосылки перемещения экстремизма из обычной жизни в виртуальный мир. Выявлено влияние экстремизма в сети на людей, а именно отрицательное воздействие на психику и мировоззрение. Объяснены причины, по которым молодежь легко поддается на экстремистские провокации.

Практически для каждого человека, имеющего дома компьютер, ежедневно посещать пространство Интернета стало обыденностью. Для многих находиться во всемирной паутине - более привычная среда обитания, нежели реальный мир. Напрашивается вопрос: что ж тут такого страшного? Разве не для упрощения нашей же жизни, а именно как наиболее удобный способ хранения и передачи информации, была создана Глобальная Сеть? Рассуждать об этом можно невероятно долго, перебивая достоинства недостатками. Но факт остается фактом: помимо создания помощи и удобства, сеть открывает большие просторы для правонарушителей, злоумышленников, экстремистов и просто хулиганов.

Нельзя отрицать, что преступность в Интернете развивается вместе с ним же и оказывает влияние на общество и отдельного человека. Это чревато многими проблемами. Одной же из таких проблем, с которыми сталкивается современное общество, является экстремизм в киберпространстве.

Экстремизм - слово не новое. В разных странах и в разные времена было дано много разных юридических и научных определений данному понятию. Тем не менее, единого же определения на сегодняшний день не существует. В общих чертах определить экстремизм можно как склонность и приверженность личности или группы лиц к крайним взглядам или действиям. В России принят Федеральный закон «О противодействии экстремистской деятельности», в котором дано определение понятию «экстремизм». Согласно этому закону, экстремистская деятельность - это деятельность, направленная на насильственное нарушение целостности Российской Федерации, создание незаконных вооруженных формирований, осуществление террористической деятельности [3]. К экстремизму можно отнести радикальные

общественные движения, а именно: террористическая деятельность, возбуждение социальной, расовой, национальной или религиозной розни и так далее.

Как же это связано с киберпространством? В данном вопросе возникает такое понятие, как киберэкстремизм. Киберэкстремизм - это экстремизм в киберпространстве. И достаточно актуальная киберугроза в наше время. Причин, вызывающих возникновение киберэкстремизма, достаточно много. Они имеют отношение к политическому состоянию страны, состоянию общества, влиянию общества на человека и многое другое. Не менее важным является социально-психологическое состояние отдельного человека, ведь, как мы знаем, даже один человек является немаловажной частью общества. Вспоминается утверждение американского математика Эдварта Нортона Лоренца: «Бабочка, взмахивающая крыльями в Айове, может вызвать лавину эффектов, которые могут достигнуть высшей точки в дождливый сезон в Индонезии» [2].

Социально-психологические причины являются одними из важнейших. Начинается все с политики. Если в стране происходит социальная дезорганизация граждан, это приводит к тому, что социум перестает существовать и функционировать как единый организм, который в свою очередь объединяет в себе общие цели, идеи, ценности. Появляются люди, некие социальные аутсайдеры, для которых возникает большая проблема - адаптироваться к новым условиям жизни. Именно эти люди вызывают возникновение и последующий рост социальной напряженности. Появляются люди, организовывающие групп, стремящиеся изменить сложившиеся порядки, не исключая возможность использования насильственных методов.

Само положение в государстве способно спровоцировать всплеск экстремистских движений. Длительно продолжающаяся социально-экономическая нестабильность в той или иной стране сопровождается с одной стороны социальной дифференциацией, растущей преступностью, жестокой борьбой за власть, с другой - низкой эффективностью работы государственного аппарата и отсутствием правовой защиты населения. Все это - предпосылки к росту попыток разрешения возникающих противоречий силовым путем, как со стороны власти, так и противопоставлено настроенных общественных групп.

Ещё одной причиной возникновения рассматриваемого движения становится так называемый мировоззренческий вакуум. Политические перевороты, революции, развития, изменения, все это и многое другое вызывает у людей девальвацию ценностей. Сложившийся мировоззренческий вакуум является показателем состояния и теоретического мышления. Общество уходит от материалистической ограниченности, хватает ума, чтобы не принимать полностью либеральные

«ценности», но и чётких представлений о «собственном, особом пути» развития нет. Зачастую это приводит к движению из крайности в крайность. Одна из таких крайностей - уже знакомый нам экстремизм [1].

Если обратиться к психологии отдельного человека, то тут можно увидеть большое количество причин, побуждающих человека к экстремистским действиям. К примеру, в голове у человека возникают фантастические идеи по усовершенствованию мира, идеи, способные улучшить и изменить положение самого общества в государстве. Но все что он ощущает - потерю способов достижения таких целей.

Немаловажным является такой фактор, как окружение человека. Саморазвитие экстремистских направленностей способно возникнуть при ослаблении внутрисемейных связей человека, при растущем чувстве одиночества, социальной заброшенности. Существуют так же такие факторы, как ощущение потери дальней перспективы, отсутствие чувства будущего, что означает снижение ответственности за свои поступки. Происходит падение нравственности, снижение ценности человеческой чести и жизни. Растет чувство беспокойства, чувство страха перед будущим и значительное психическое напряжение.

С привычкой оглядываться на других людей, и что происходит вокруг, человек способен замечать вещи, не дающие ему покоя. Бесцеремонное, порой провоцирующее поведение членов новой элиты, широко распространенная реклама товаров и услуг, которые являются явно недоступными для подавляющей части населения, рост силы попкультур, транслируемой субкриминальным шоу-бизнесом. Этот ряд факторов способен вызвать социальную фрустрацию у отдельной личности, то есть состояние гнетущего напряжения и тревожности, безысходности и отчаяния, в связи с невозможностью удовлетворения своих разнообразных желаний и потребностей.

К тому же, в рассматриваемом вопросе не стоит забывать об этническом предпринимательстве. Вышесказанное понятие подразумевает под собой крупное освоение территорий под собственные экономические уклады и интересы отдельных этнических меньшинств. Миграции народов, их способность к достаточно быстрой адаптации и поиску места в экономический нише той или иной страны порой естественно вызывает различные оценки таких процессов у коренного населения. Эти оценки далеко не всегда положительны. У части населения возникают возмущения, относительно широкого развития иностранных мигрантов. Это становится предпосылками к националистическому экстремизму, который в свою очередь успешно прячется за патриотизм [4].

В общем-то, не только то, что мигрирующие этносы находят и занимают определенную нишу в экономике страны, способствует воз-

мущениям у некоторых людей. Сама миграция этих людей, в первую очередь из регионов Закавказья и Средней Азии, на территорию страны вызывает обострение националистических настроений. Такие потоки разрушают, исторически сложившийся этнический баланс населения и деструктивно влияет на межэтнические отношения. Происходит это хотя бы потому, что часть населения зачастую хотят, но не могут трудоустроиться, найти свое место в жизни. Естественно, что появление все большего числа конкурентов их совсем не радует. Да и то, что часть мигрирующего населения не желает зарабатывать законными способами и создает этнические преступные группировки, что естественным образом вызывает ещё большее недовольство среди населения.

Так почему же экстремистские группировки выходят на новый уровень - перемещаются в виртуальную сеть?

Ответ на этот вопрос состоит из нескольких частей. Одной из причин является то, какую целевую аудиторию можно встретить в сети.

На просторах всемирной паутины чаще всего можно встретить молодежь. Именно они является добычей экстремистских группировок в сети. Молодые люди, обитающие в киберпространстве, наиболее максимально подходят для усвоения экстремистских идей. Подростковый возраст, от 14 до 22 лет считается максимально уязвимым в этом плане. Молодежное сознание и без того переменчиво, в силу отсутствия жизненного опыта и знания, и сопровождается достаточно резким критическим отношением к обществу и положением в нем. Представление об общественных ценностях и нормах имеет достаточно смутное представление. Они полны внутреннего протеста. Такие люди готовы психологически к усвоению экстремистских идей.

Основываясь на данных Интернет-статистики, именно дети и подростки, попадая в Глобальную сеть, оказываются в зоне риска [8]. На открытых и доступных форумах они обсуждают, как совершать самоубийства и убийства, вступают в экстремистские сообщества и получают доступ к жестоким онлайн играм. Разве не подростковый максимализм и отсутствие четкого осознания себя и своего места в обществе является крупной мишенью для киберэкстремистов?

Об опасности киберэкстремистских сообществ могут свидетельствовать различные случаи, прогремевшие в разных уголках планеты. Одним из таких случаев проявления агрессии, связанной с Интернетом, является ситуация, прогремевшая в Америке 22 марта 2005 года. Шестнадцати летний житель индейской резервации штата Миннесота Джефф Вейзи застрелил девять человек, включая членов своей семьи и одноклассников. К тому же, ещё семь учеников были ранены. Следователями было установлено, что подросток совершил убийства из-за серьезных психологических проблем. Он был чем-то вроде отщепенца

среди окружавших его людей. Из-за неудачных попыток найти свое место в жизни, из-за отсутствия нормального общения со сверстниками и по причине замкнутости характера, он предпочитал находить общения в Интернете, проводя время на различных праворадикальных сайтах и пронацистских форумах под никами Todesengel (Ангел смерти) и NativeNazi (Местный нацист). Подросток восхищался Гитлером и идеологией нацизма [8].

Этот далеко не единичный случай экстремисткой деятельности подростка, получившего «вдохновение» от Интернета подтверждает уязвимость молодежи в Глобальной сети.

Да и ещё одна причина, почему подростки попадают в экстремистские группы, достаточна, проста и примитивна. Искренне верить в то, что ребенок в поисках обычно реферата по истории не наткнется, а если наткнется, не поинтересуется, на наркотики или предложения сделать взрывчатку, было бы очень наивно. Зачастую именно темная сторона Интернета привлекает детей, хотя бы просто потому, что запретный плод сладок.

Были выделены признаки, по которым можно разглядеть влияние киберэкстремизма на подростка:

– манера поведения становится значительно более резкой и грубой;

– резко изменяется стиль одежды и внешнего вида, соответствуя правилам определенной субкультуры;

– на компьютере оказывается много сохраненных ссылок или файлов с текстами, роликами или изображениями социально-экстремального содержания;

– в доме появляется непонятная и нетипичная символика или атрибутика (как вариант – нацистская символика), предметы, могущие, быть использованы как оружие;

– резкое увеличение числа разговоров на политические и социальные темы, в ходе которых высказываются крайние суждения с признаками нетерпимости;

– псевдонимы в Интернете, пароли и т.п. носят экстремально-политический характер [7].

Но уязвимость подростков не единственная причина, почему экстремистские группировки ищут и вполне успешно находят себе место в сети.

Интернет в первую очередь доступен. Кто угодно может разместить любую информацию. Возможность создания экстремистских интернет-сообществ сложно пресечь. К таким сообществам относятся: экстремистские религиозные секты; группы политических и экономических террористов; традиционные и ново организованные преступ-

ные сообщества и так далее. Киберпространство дает личности гораздо большую свободу действий, чем реальная.

Не менее важным фактором является высокая степень анонимности. Четких ограничений по количеству потенциальных участников нет, в работе групп могут принимать участие сколько угодно человек, при чем, это могут быть пользователи, находящиеся в абсолютно разных географических точках земного шара.

Виртуальная среда создает удобные условия для возникновения таких сообществ. Сейчас был «забанен» в сообществе пользователь, пропагандирующий экстремистское движение - через час он уже регистрируется под новым «ником», с новыми данными и продолжает свою деятельность. Сегодня было заблокировано экстремистское сообщество - а завтра оно создается заново и собирает свою публику. Попытка поймать пропагандиста заканчивается ничем: вот он оставлял сообщения, побуждающие и призывающие к подобного рода деятельности, через короткий промежуток времени сообщения удалены и самого пользователя не существует. Это все достаточно тонко и неуловимо.

Да и отсутствие цензуры тут не маловажно. Большинство сайтов и форумов предусматривают возможность оставлять анонимные сообщения. Можно оставить сообщение с определенной ссылкой, которое успеет привлечь внимание психологически готовых к усвоению подобных идей людей, и никто не узнает человека, что это сообщение оставлял.

Несомненным преимуществом, которым пользуются группировки экстремистов для вербовки новых сторонников и распространения пропагандистских материалов, является и то, что не так уж и просто определить реальное количество подобного контента. Чаще всего, сторонний наблюдатель и не осознает, что какая-либо информация в Интернете, на которую он ненамеренно наткнулся, имеет экстремистский подтекст. Для непосвященных людей такие переговоры могут показаться чем-то обыденным и не вызвать никаких подозрений.

Экстремистам очень удобно общение посредством Интернет-сайтов, общественных и политических форумах, в сфере блогов. Эти сайты способны «хоститься» в доменной зоне любой точки земного шара. В Интернет-среде не сложно назначение акций различного рода. Воспользоваться они могут обычной рассылкой, которая достигает как настоящих и потенциальных участников, так и обычных пользователей. «Опытные» киберэкстремисты делятся своими знаниями с новичками, дают советы, как правильно и грамотно организовать акцию, как поступить на каждой её стадии и непосредственно после акции. Иногда даже учат тому, как организовывать провокации. Всё это очень удобно, не правда ли?

Хитрость и ловкость группировок экстремистов способна удивлять. К примеру, в Чечне кибертеррористы умудрились сформироваться даже при отсутствии телекоммуникационной инфраструктуры. А именно, обучая молодых людей и побуждая их на развитие компьютерных навыков, предполагая использовать их умения в борьбе с федеральным центром. Преступникам более старших возрастов было проблематично овладевать техническими средствами кибертерроризма. Именно поэтому они используют для этой цели именно молодежь.

Но не стоит утверждать, что абсолютно все приверженцы экстремизма в сети настроены агрессивно и негативно. Часть молодых людей, вступающих в такие группировки, зачастую уверены что занимаются чем-то вроде очистки страны от проблем. Беспокоящими их проблемами являются несправедливость формирования элит, безработица, бедность, несправедливость при оплате труда и карьерном росте, стесненные социальные обстоятельства, высокий уровень преступности, отсутствие правосудия в интересах рядового гражданина, невозможность влиять на политическую систему путем легальных политических механизмов, неадекватность государственного регулирования. У многих людей, преимущественно у молодежи, возникает желание сделать мир гораздо более справедливым, чем он есть. Просто они не сразу осознают, что такой быстрый, простой и понятный путь, как экстремизм, не является самым лучшим.

Порой удивительно, как же экстремисты достигают такого успеха в увеличении своей численности. Для этого они используют несколько приемов, обращенных на психологическое воздействие на человека. И человек, сам того не ведая, ведется на провокацию. Наиболее часто используется заведомо ложное истолкование истории. Этот способ наиболее применим к национальному экстремизму [9]. Суть - в постепенном изменении общественного мировоззрения. Искажение хронологий исторических дат, искажение событий дает возможность воздействовать на людей нужным для экстремистов образом. Не менее важное влияние оказывает воздействие на людей с помощью подставных видео роликов с якобы «мест боевых движений». Да и используется элементарный метод - глобализация. Гораздо проще убедить в важности противостоянию так называемому врагу, если правильно описывать его негативные черты.

Киберэкстремизм - проблема достаточно актуальная для настоящего времени. Попытки бороться с ней чаще всего терпят неудачу. Зачастую принимаются попытки законодательно регулировать движение экстремизма в сети. Но этот способ вряд ли будет являться эффективным.

Можно ли сказать, что однажды рост и развитие экстремизма в сети прекратиться? Вряд ли, ведь возможности к девиантному поведе-

нию в сети развиваются вместе с самой сетью. Киберэкстремизм - это не единичный случай. Методы совершенствуются, социальные предпосылки для присоединения к подобному движению всегда будут окружать члена общества, хотя бы потому, что достичь стабильности в государстве и в собственном окружении практически невозможно. Да и с учетом порой сильного, но незаметного напора на психологические и мировоззренческие качества человека, сложно сказать, что проблема киберэкстремизма рано или поздно перестанет расти. Остается надеяться, что людей, не поддающихся влиянию экстремистов в сети, будет не меньше, чем самих киберэкстремистов.

Публикация выполнена в рамках работы над проектом РГНФ № 13-06-00156 «Подготовка педагогических кадров к профилактике и противодействию идеологии киберэкстремизма среди молодежи».

Библиографический список

1. Журавлев В.И., Эпистемологические и мировоззренческие аспекты теоретико-вакуумной репрезентации реального мира [статья] - Донецк, 2005. (дата обращения: 03.05.2013)

2. Живая библиотека [информационный сайт]. URL: http://www.livelib.ru/ (дата обращения: 03.05.2013)

3. Информационно-правовой портал «Гарант» [информационный сайт]. URL: http://www.garant.ru/ (дата обращения: 03.05.2013)

4. Исаева М. Предпосылки и источники молодежного экстремизма [статья] - М., 2007 (дата обращения: 03.05.2013)

5. Российский Фонд Развития Высоких Технологи [информационный ресурс]. URL: http://www.dvpt.ru/ (дата обращения: 03.05.2013)

6. Экстремизм [информационный сайт]. URL: http://www.ekstremizm.ru/ (дата обращения: 03.05.2013)

7. Центр Безопасного Интернета России [информационный сайт]. URL: http://www.saferunet.ru/ (дата обращения: 03.05.2013)

8. Центр исследования компьютерной преступности [информационный сайт]. URL: http://www.crime-research.ru/ (дата обращения: 03.05.2013)

9. Центр «Молодежные инициативы» [информационный сайт]. URL: http://molinfocenter.ru/ (дата обращения: 03.05.2013)

Боброва И.И.
к.п.н., доц. каф. прикладной информатики

ПСИХОЛОГО-ПЕДАГОГИЧЕСКАЯ БЕЗОПАСНОСТЬ ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ

ФГБОУ ВПО «Магнитогорский государственный университет»,
Friend_bi@mail.ru

Аннотация

В статье рассмотрены некоторые риски, присутствующие в образовательной среде учебного заведения; особенности формирования комфортных психолого-педагогических условий виртуального взаимодействия студентов и преподавателей; даны обоснования и рекомендации по использованию сетевого этикета.

Современное образование ассоциируется не только с традиционными формами обучения, но и виртуальным пространством каждого образовательного учреждения. Вследствие использования современных информационных технологий изменились: деятельность обучаемых и обучающихся; содержание образования в традиционной образовательной системе. Главная причина этого явления в том, что образовательный процесс – это, прежде всего информационное взаимодействие между организаторами этого процесса и теми, на кого он направлен. В рамках этого взаимодействия происходит поиск, накопление, обработка и хранение информации. В силу этого обстоятельства среду, в которой он протекает, рассматривают в качестве информационной образовательной среды.

Любая информационная среда образовательного учреждения имеет ряд признаков и свойств:

1. Представляет собой одну из предложенных моделей: «человек-техника», «человек-человек», «человек-знаковая система», «человек- художественные образы». Какая бы модель ни была реализована в каждом конкретном случае, все они направлены на совершенствование человеческой личности, невозможны без эмоционального проживания ситуаций и ориентированы на социально-значимую цель.
2. Обладает свойствами системы и развивается как открытая самоорганизующаяся система по собственным закономерностям в непрерывной зависимости от особенностей педагогической системы учреждения.
3. Саморазвитие системы предполагает совершенствование ее уровня организации и наращивание технической мощи системы.
4. Концептуальное целеполагание накладывает на образовательную систему необходимость координации действий участников процесса в достижении единой цели обучения. Но с учетом конкретных обстоятельств достижение единой цели трансформируется в последовательность уникальных локальных задач, решаемых каждым педагогом и слушателем на каждом этапе образовательного взаимодействия (образовательную; управленческую; коммуникационную).

В любой образовательной системе можно обнаружить разноплановые и разнообразные риски и угрозы. Для начала напомним некоторые термины. «Комплексная безопасность образовательного учреждения – состояние защищенности образовательного учреждения от реальных и прогнозируемых угроз социального, техногенного и при-

родного характера, обеспечивающее его безопасное функционирование». «Комплексная безопасность образовательной среды – совокупность определенных видов безопасности (интеллектуальной, духовной, нравственно-этической, психологической, педагогической, этнической, физической, трудовой, управленческой), гарантированно обеспечивающая защищенность всех участников образовательного процесса». Попробуем разобраться с некоторыми угрозами и рисками, присущих образовательной среде. Выявление их позволит нам создать комфортные психологически безопасные условия существования виртуальной образовательной среды.

Выявление рисков позволит нам интерпретировать эти явления на субъект-субъектном и субъект-объектном уровне.

Выявляя риски в образовательной среде, мы сможем проанализировать психологическую составляющую данного феномена. В педагогических исследования риск трактуется "...как состояние, связанное с необходимостью совершать некоторые действия, поступки в ситуации с неоднозначным исходом. Чем выше риск, тем выше вероятность неудачного развития событий". Успех работы, а значит и качество результата образовательной системы во многом зависит от правильной оценки рисков и организации действий, направленных на их снижение. С учетом объективных условий, желаемых и ожидаемых результатов обучения, можно классифицировать риски по разным признакам. Выделим некоторые проблемные направления:

1. Риски, связанные со слушателем (студентом).

2. Риски, связанные с преподавателем.

3. Риски, связанные с управлением виртуальной образовательной средой.

4. Риски, связанные с организацией учебно-воспитательного процесса и содержанием образования.

Результаты опроса, проведенного в рамках круглого стола, показали % количества упоминаний от общего числа участников [12]:

1. Риски, связанные со слушателем (студентом):

- отклонение от нормы психического и физического развития – 60%;
- низкая мотивация – 35%;
- трудности адаптации – 30%;
- высокий уровень агрессии – 20%;
- педагогическая запущенность – 20%;
- учебная перегрузка – 20%;
- личностные особенности – 10%;
- страхи, тревожность – 10%.

2. Риски, связанные с преподавателем:

- эмоциональное выгорание – 55%;
- некомпетентность – 30%;

- низкий уровень мотивации – 20%;
- низкий уровень профессионального саморазвития – 20%;
- большая учебно-воспитательная нагрузка – 15%;
- большая наполняемость классов – 10%;
- повышенная ответственность, тревожность – 10%;
- пожилой возраст – 10%;
- негативные стереотипы, связанные с неуспевающими детьми – 10%;
- завышенная требовательность – 5%;
- грубость, безразличие – 5%;
- соматические заболевания – 5%;
- неудовлетворенность социальным статусом – 5%;
- дезадаптация – 5%;
- негибкость, ригидность мышления, авторитарность – 5%.

3. Риски, связанные с управлением виртуальной образовательной средой:
- управленческая некомпетентность – 45%;
- личностные особенности и авторитаризм директора – 30%;
- отсутствие команды единомышленников в администрации – 10%;
- неадекватность и несоответствие предъявляемых требований возможностям педагогического коллектива – 10%;
- формализм, закрытость администрации – 5%;
- введение инноваций – 5%;
- процедура аттестации – 5%;
- изменение состава администрации, изменение профиля школы – 5%;
- проблемы самофинансирования – 5%;
- нездоровая соревновательность – 5%;
- отсутствие мотивации повышения квалификации педагогического коллектива – 5%.

4. Риски, связанные с организацией учебно-воспитательного процесса и содержанием образования:
- большой объем учебной нагрузки – 20%;
- не рецензируемые учебники – 20%;
-невнимание к эмоциональной сфере ребенка, психо-эмоциональные перегрузки учащихся – 20%;
- завышенные требования при аттестации (ЕГЭ) – 15%;
- сложность учебных программ – 15%;
- излишняя рационализация образования – 10%;
- необходимость адаптации учебно-воспитательных программ – 10%;
- введение новых предметов – 10%;
- модернизация образования – 10%;
- недостаток развивающих программ – 10%;
- введение профильного обучения – 5%;
- переход на триместры, изменение расписания – 5%;

- несоответствие нормативно-правовой документации укладу жизни школы – 5%;
- отсутствие индивидуальной работы с детьми – 5%;

Данные результатов опроса педагогов-психологов, позволили конкретизировать виды рисков в образовательной среде, нарушающих психологическую безопасность и определяемых как внешними, так и внутренними условиями.

Анализируя результаты, собранных статистических данных, полученных в результате опроса разных категорий участников образовательного процесса и в разных образовательных организациях, психологи (педагоги) установили, что наиболее широко распространенными получились риски, связанные с отклонением от нормы психического и физического развития (60%), на втором месте - низкая мотивация учения (35%) и трудности адаптации (30%). Побочным явлением отсутствия мотивации к обучению стало появление огромного числа межличностных конфликтов между слушателями и между слушателями и педагогом. По второй группе рисков на первом месте оказалось явление - эмоциональное выгорание педагогов(55%), следом - их некомпетентность (30%), низкий уровень мотивации творческой деятельности (20%) и низкий уровень профессионального саморазвития педагога (20%). Как следствие, это так же приводит к появлению конфликтов между студентами, так и между студентом и преподавателем которые выражаются в отсутствии доверительных отношений и психологической поддержки, авторитарности, нетерпимости и низкой коммуникативной компетентности.

Для формирования психосоциального благополучия среды может выступать ее психологическая безопасность.

Под «психологической безопасностью образовательной среды» мы понимаем ее состояние, свободное от проявлений психологического насилия во взаимодействии, способствующее удовлетворению потребностей в личностно-доверительном общении, создающее референтную значимость среды и обеспечивающее психическое здоровье включенных в нее участников".

Для обеспечения психологической безопасности образовательной среды необходимо выявить уровень психологического насилия. Современное образование не является безопасным. Традиционное образование изначально базируется на постулатах: дисциплина; учебный план; нормы; правила..., это давление не только на личность ребенка, но и на взрослого (педагога). Иногда насилие становится нормой поведения некоторых взрослых (педагогов) в образовательной среде. А это плохой пример модели поведения, который ребенок может перенести на вне учебную жизнь.

Психологическую безопасность образовательной среды, влияет на психосоциальное благополучие не только студентов, но и остальных участников образовательной среды – преподавателей, сетевых администраторов.

Единое образовательное пространство создается, опираясь на концепции образования общества, на образовательную политику учреждения, не нарушая психологические состояние всех участников учебного взаимодействия.

В одних источниках «безопасность – это качество какой-либо системы, определяющее ее возможность и способность к самосохранению». В других – «это система гарантий, обеспечивающих устойчивое развитие и защиту от внутренних и внешних угроз. Большинство определений подтверждают, что безопасность направлена на сохранение системы, на обеспечение ее нормального функционирования». На основании этих фактов мы будем рассматривать психологическую безопасность образовательной среды как условие, при котором гарантированно будет достигнуто высокое качество знаний, устойчивая мотивация учения.

Среди главных угроз, существующих в образовательной среде, мы выделяем: психологическое давление (насилие); неудовлетворенность в доверительном общении между педагогом и слушателем; низкое качество наполняемости образовательной среды.

Выделим три аспекта психологической безопасности образовательной среды:

-образовательная среда без психологического давления (насилия) в процессе обучения, в которой решена проблема, личностно-доверительных отношений при общении; которая обеспечивает психологическое здоровье и уважение всех ее участников;

-образовательная среда, вызывающая чувство гордости у участников процесса, благодаря принадлежности к референтной группе, которая дает чувство защищенности системы от внешнего проявления;

-образовательная среда, развивающаяся в направлении предотвращения угроз, использующаяся, в том числе и для продуктивного устойчивого развития личности.

Психологическая безопасность образовательной среды, обеспечивающая микро социальное окружение, свободное от психологического насилия, определяющая ее референтную значимость, удовлетворяющая основные потребности в личностно-доверительном общении, определяет динамическое равновесие между человеком и социальной средой в сторону повышения психического здоровья личности, его психосоциального благополучия. Данное положение получило экспериментальное подтверждение в наших исследованиях [Баева, 2002;

2006]. Психологическая безопасность образовательной среды отражается в характеристиках защищенности ее субъектов, которая проявляется в показателях психического здоровья и уровне его психосоциального благополучия.

Меры, предпринимаемые для поддержания психического здоровья участников образовательного процесса и психосоциального благополучия, нам видятся в следующем:

- запуск и поддержание процессов саморазвития;
- помощь в планировании жизненного пути и профессионального самоопределения;
- развитие способности к само регуляции и самоуправлению поведением;
- профилактика социальных опасностей (употребление наркотиков, вербовка в деструктивные культы и т.п.)

Обеспечение безопасности образовательной среды возможно благодаря системному мониторингу образовательной среды, который позволяет своевременно выявить возникающие угрозы и риски опасности образовательной среды и провести соответствующие эффективные коррекционные мероприятия.

Мониторинг образовательной среды способен решить следующие задачи:

- выявить угрозы и риски, появляющиеся в образовательном процессе учебного заведения;
- разработать комплекс критериев и показателей, оценивающие состояние образовательной среды учебного заведения (количественные и качественные показатели);
- упорядочивание информации и работе системы; диагностика и анализ ее содержания;
- визуализация полученных результатов диагностики образовательной среды;
- информационное сопровождение, анализ состояния системы и прогнозирование перспектив развития безопасности образовательной системы; выработка и реализация принятых решений.

Если следовать за А. Маслоу, который отмечал, что среда должна быть подобна доброму наставнику, то в безопасности образовательной среды на первый план выступает проблема именно самого такого «доброго наставника», руководящим фактором педагогического поведения которого, на наш взгляд, выступает уровень сформированности у него психолого-педагогической культуры. Самого термина «психолого-педагогическая культура» в научном обороте, по существу, нет. В словарях, научных публикациях широко используется термин – педагогическая культура. В словарях практически отсутствует, но в научном обороте стал встречаться, термин – психологическая культура,

есть попытки его определения (В.М. Аллахвердов, Н.В. Беляк, А.А. Бодалѐв, М.В. Иванов, Е.А. Климова, К.С. Колмогорова, А.Б. Орлова, и др.).

Представляется, что в свете безопасности образовательной среды необходимо разрабатывать значимость психолого-педагогической культуры, прежде всего, педагогов и студентов, определяющих общую направленность и степень безопасности/опасности образовательной среды и ввести в оборот термин педагогическая безопасность образовательной среды.

Педагогическая безопасность образовательной среды, на наш взгляд, – это такое ее состояние, в котором безопасность и удовлетворенность ею всех участников определяется наличием у субъектов, организующих образовательный процесс и образовательную среду, психолого-педагогической культуры и умений реализации технологий гуманной педагогической деятельности в соответствии с интересами каждой личности и общества в целом. Психолого-педагогическая культура – это совокупность общей культуры, личностных качеств педагога, ориентированных на гуманное осознание и реализацию педагогической деятельности на основе глубокого понимания психики окружающих людей и своей собственной, профессиональной компетентности и педагогического мастерства, порождающая состояние внутренней профессиональной удовлетворенности и психологического благополучия.

Педагогическая компетентность по определению. М. Митиной включает в себя знания, умения, навыки, а также способы и приемы их реализации в деятельности, общении, развитии (саморазвитии) личности.

Определяя психологическую и педагогическую безопасность образовательной среды, предполагаем, что в педагогической парадигме не снимаются такие явления, как:

- насилие самого факта образования;

- насилие из-за противоречия: свободы и ограниченности выбора в условиях образования;

- стремление к самоутверждению и самореализации всех участников образования и реальной неспособности это осуществить в полной мере из-за чрезмерной интенсификации и стимуляции образовательной среды (высокие требования, объем и сложность информации, темп еѐ освоения и жесткое сроки обучения и его организации, недооценка (или завышенные требования) педагогами и родителями возможностей воспитанника, отсутствие достаточных способностей и у тех, и у других; превосходство других, завышенные амбиции, недостаток психических и физических возможностей у самого воспитанника и взрослого окружения).

Преподаватель, у которого сформирована психолого-педагогическая культура, сумеет не только гуманно выстроить систему отношений в образовательной среде, но и выбрать и осуществить такую технологию педагогической деятельности, которая позволит несмотря на изначально насильственную природу образования, ограничивающей и педагога, и обучаемых в этом пространстве, максимально ее смягчить. Решение этого вопроса следует начинать с формирования сетевого этикета между участниками образовательного процесса.

«Этикет – часть социального уровня культуры» [А.Л. Гусейнов] Поскольку неотторжимой частью культуры является система цензур и запретов, то можно сказать, что этикет на обыденном уровне является отражением общего ее состояния. В процессе любого общения есть определенные границы, так называемые гласные и негласные правила. Начинаются правила этикета с традиции, и во многом сохраняют с ними связь. Известный российский этик Р.Г.Апресян пишет, что « … выполнение обряда или какого-либо ритуала выделяет и обеспечивает принадлежность участников церемонии к некоему сообществу, их пристрастие неким высшим смыслам, а правилами этикета задаются рамки обычного социального взаимодействия» [1, с. 18].

Одна из особенностей общения – это постоянное межличностное взаимодействие с участниками процесса, т.е. традиционно – студентов и преподавателей, а ввиду изменяющейся коммуникативной среды учебных заведений – с компьютерными специалистами (технический персонал, администратор локальной сети, администратор, редактор или дизайнер веб-сайта, Интернет-провайдер).

Современный человек должен обладать определенным набором умений и навыков, уметь строить эффективную коммуникацию с другими людьми, непосредственно участвующими в общении, и поддерживающих, администрирующих процесс в электронной среде (администраторы, технический персонал). Аналогично, студенту, преподавателю необходимо уметь строить свою коммуникацию с другими участниками процесса общения в целях учения, самообучения – с одноклассниками, преподавателями, а также с техническим персоналом, администратором. Получение и развитие этих навыков возможно только в ходе активной деятельности, включающей разнообразные формы компьютерно-опосредованной коммуникации (межличностная, групповая, межкультурная) [10].

Чаще всего нет сформированной практики использования компьютерными коммуникациями; нет пособий по коммуникациям в электронной среде, поэтому каждый участник компьютерного взаимодействия получает эти коммуникативные навыки путем подражания действиям пользователей, которых считают более компетентными в меж коммуникационных технологиях, в образовательном процессе,

наблюдая за ними (в том числе за преподавателем, тьютором) в ходе обучения.

В последние годы, в особенности за рубежом, было опубликовано большое количество статей, посвященных проблемам взаимодействия человека с глобальными компьютерными сетями. Правда, этическим аспектам этого взаимодействия в этих публикациях должного внимания не уделяется.

Говоря об этике Интернета, принято считать ее продолжением академического направления компьютерной этики, которая, с была рассмотрена и изложена в работах В. Мэнера. По его мнению сетевая этика "...представляет собой область прикладной этики, изучающую этические проблемы, «усугубляемые, трансформированные или же созданные компьютерными технологиями». Такой подход, опирающийся на труды классиков данного направления, Н. Винера и Дж. Вейценбаума, представлен в работах Дж. Мура, Д. Джонсон, Дж. Снэппера, И. Ю. Алексеевой, И. Л. Галинской и др., и представляется вполне правомерным, если рассматривать Интернет в качестве средства коммуникации (т. е. медиа), и, следовательно, обращать первоочередное внимание на опосредованный характер виртуального взаимодействия [4,11].

По другому мнению, этику виртуальной коммуникации следует рассматривать в качестве одной из разновидностей профессиональной этики, содержательно наиболее близкой профессиональной этике библиотекаря и журналиста. Этот подход строится на основании анализа наиболее распространенных и общественно-значимых видов деятельности Интернет-пользователей, и поэтому, хотя и с определенными оговорками тоже имеет право на существование.

Под сетевым этикетом понимаются правила поведения, общения в Сети, традиции и культура интернет-сообщества, которых придерживаются большинство, это понятие появилось в середине 80-х годов XX века в эхо-конференциях сети.[7]

Анализ научной литературы [5,8] показал, что в «сети» важной проблемой является тот факт, что вместо известных психологических механизмов воздействия на человека (внушение, убеждение, заражение, подражание), все они применяются в образовательном процессе, наиболее часто применяемым методом является метод - «убеждения». В виртуальной образовательной среде к "убеждению" добавляются механизмы «заражения» и «подражания».

В научно-педагогической литературе уже накоплен некоторый опыт преодоления проблем компьютерно-опосредованной коммуникации в электронной среде образовательным сообществом. Появились правила норм и правил сетевой этики, которые предполагают и зачастую обеспечивает взаимно-ожидаемые способы поведения участников

учебного взаимодействия. Как следствие, получение ожидаемых результатов при взаимодействии в малых группах приобретает организованный и взаимосогласованный характер.

Так, например, в исследованиях О.В. Лутовиновой [6] по вопросам сетевой этики, основанной на перекрещивании норм поведения, характерных для трех пересекающихся групп – сообщества пользователей Интернет, образовательного и делового сообществ. Компьютерная этика для профессионалов и пользователей при решении моральной дилеммы определяется следующим, каким этическим принципам следовать, каким из них отдать предпочтение при использовании ИКТ в своей деятельности. Современная виртуальная среда может содержать специальный инструментарий для содействия эмоциональным коммуникативным связям и отношениям.

Таким образом, образовательная среда Интернета предоставляет широкие возможности для любого рода взаимодействия и дает свободу полную свободу самореализации. Но при этом процесс взаимодействия, сопровождается потерей настоящего имени, человеческой оболочки (тела), социального статуса, литературной (научной) речи. Личность при таком общении приобретает несуществующие черты, становиться виртуальной. Это приводит к изменению личности. И это дает некоторым авторам основание утверждать, что в современном обществе «сущность человека отчуждается не в социальную, а в виртуальную реальность»[9].

Как показал, анализ методических публикаций наиболее полному решению проблемы оптимизации организации учебной деятельности в обучении способствуют знания о культурном общении в Интернете, сетевого этикета [3].

В современных условиях выделяют специфичные элементы сетевого этикета («netiquette» – «нетикета»), обусловленные форматом данного вида общения, активно проникают в живую повседневную речь. Действительно, непрерывный рост информации накладывает отпечаток не только на характер организации письменно-печатной продукции, но и на манеру подачи информации в устном общении. Интернет и СМС коммуникация, ярко демонстрирующие признаки живого устного общения, предстают актуальным материалом для исследования и в силу роста своей популярности [2].

В МаГУ уже несколько лет работает виртуальный портал, который служит источником учебной информации, способом общения между преподавателем и студентом. Традиционное образование как таковое видоизменилось, взяв некоторые формы дистанционного образования. Для успешной реализации этой новой формы все участники образовательного процесса должны обладать определенным набором коммуникационных компетенций, понимать наличие некоторых угроз

и рисков, появившихся в результате использования сетевых технологий и при этом знать, что самый простой способ комфортной работы в образовательной среде – это соблюдение сетевого этикета всеми участниками этого процесса.

Публикация выполнена в рамках выполнения проекта РГНФ № 11-06-01006 «Разработка и апробация модели подготовки научно-педагогических кадров к обеспечению информационной безопасности в ИКТ - насыщенной среде».

Библиографический список

1. Буторина Е.А. Особенности коммуникации на естественном языке в Internet. 2000. [Электронный ресурс]. Режим доступа - http:www.dialog-21.ru /Archive /2000/ Dialogue.

2. Гусейнов Г. Другие языки. Заметки к антропологии русского интернета: особенности языка и литературы сетевых людей. 2000. [Электронный ресурс]. Режим доступа – http://nlo.magazine.ru/dog/tual/main8.html

3. Дацюк С.А. Парадоксальная интенция свободы в Internet. – 1997. [Электронный ресурс]. Режим доступа – http://www.uis.kiev.ua/russian/win/~xvz/par int.html.

4. Конецкая В.П. Социология коммуникации. – М.: Междунар. Ун-т Бизнеса и Управления, 1997. – 9 с.

5. Литневская Е.И. Об Интернете и так называемой «порче языка» // Русский язык: исторические судьбы и современность: III Международный конгресс исследователей русского языка. – М., 2007. – 393-394 с.

6. Лутовинова О.В. Современный виртуальный креатифф: о некоторых особенностях языка Рунета // Русский язык: исторические судьбы и современность: III Международный конгресс исследователей русского языка. – М., 2007. — 394 с.

7. Нестеров В.В. К вопросу об эмоциональной насыщенности межличностных коммуникаций в Интернете. [Электронный ресурс]. Режим доступа – http:// flogiston.ru/projects/articles.

8. Носов Н.А. Виртуальная психология. – М.: Аграф, 2000. – с.432

9. Пашковская К. Лингвистические аспекты виртуальной коммуникации, [Электронный ресурс]. Режим доступа – http://www.volny.edu/soclab/students/papers/chats.php

10. Рогов Е.И. Психология общения. – М.: Владос, 2003.

11. Травин А. Виртуальная коммуникация как синтез письменной и устной речи № 7-8// Мир Internet. 1999.

12. Безопасность образовательной среды: сб. ст./ Отв. ред. и сост. Г.М. Коджаспирова. – М.: Экон-Информ, 2008, – с. 158.

Гаврилова И.В.
к.п.н., доц. каф. информационных систем

ПРОФИЛАКТИКА КИБЕРЭКСТРЕМИЗМА СРЕДИ МОЛОДЕЖИ

ФГБОУ ВПО «Магнитогорский государственный университет»,
ipopova@masu-inform.ru

На современном этапе развития информационного общества в России обостряется проблема молодежного киберэкстремизма, обусловленная рядом факторов. Во-первых, это становление и развитие российского терроризма и экстремизма на весьма благоприятном криминогенном фоне. Во-вторых, рост ИКТ-грамотности среди населения. В-третьих, психологические особенности молодежи как возрастной группы.

В общем смысле под киберэкстремизмом понимают экстремизм в виртуальном (кибер-) пространстве. В свою очередь, экстремизм толкуется как приверженность к крайним взглядам мерам, наиболее часто проявляемым в политике, международных отношениях, религии и т.д. В России юридическое определение того, какие действия считаются экстремистскими, содержится в статье 1 Федерального Закона № 114-ФЗ «О противодействии экстремистской деятельности». Федеральный закон от 27 июля 2006 г №149 – ФЗ «Об информации, информационных технологиях и о защите информации» устанавливает запрет на распространение информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная ответственность. Президент Института религии и политики А. Игнатенко обращает внимание на то, что количество сайтов, которые распространяют идеологию экстремизма, достигает 10 тысяч[1].

Как отмечают ученые, киберэкстремисты используют компьютерные сети (чаще всего Интернет) для пропаганды своих взглядов, вербовки сообщников, сбора пожертвований, размещения руководств по организации терактов, психологического терроризма, сбора информации о предполагаемых целях и объектах шантажа, подготовки террористов, пропаганды расовой, религиозной и других форм нетерпимости. [4]. По данным ВЦИОМ 70% самых активных пользователей «всемирной паутины» (т.е. те, кто пользуется Интернетом ежедневно) - это население в возрасте от 18 до 24 лет[2]. Это значит, что основная

[1] http://www.interfax-religion.ru/?act=print&div=9859
[2] http://www.bizhit.ru/index/vozrast_veb_polzovatelej/0-240

аудитория, которая ежедневно сталкивается с экстремизмом в глобальной сети, – молодежь.

В соответствии со Стратегией государственной молодёжной политики в Российской Федерации, утверждённой распоряжением Правительства Российской Федерации от 18 декабря 2006 года N 1760-р, к категории молодёжи в России относились граждане от 14 до 30 лет. С точки зрения социологии молодежь – поколение людей, проходящих стадию социализации. Она активно осмысляет культурные и политические явления, исходя, прежде всего из своего жизненного опыта и сформировавшихся ценностных установок. По мнению Карла Мангейма, «молодёжь ни прогрессивна, ни консервативна по своей природе, она — потенция, готовая к любому начинанию. У молодежи еще нет закрепленных законом интересов ни экономических, ни ценностных, имеющихся у большинства взрослых людей. Этим объясняется тот факт, что в юности многие действуют как ревностные революционеры или реформаторы, а позднее, получив постоянную работу и обзаведясь семьей, переходят в оборону и выступают за сохранение status quo. На языке социологии быть молодым означает стоять на краю общества…» [2]. В своих оценках молодежь зачастую не приемлет полутонов, а, значит, мыслит граничными категориями, характерными для экстремистских взглядов. Как результат, экстремизм в молодежной среде проявляется в деформациях сознания, в увлеченности националистическими, неофашистскими идеологиями, нетрадиционными для Российской Федерации новыми религиозными доктринами, в участии в деятельности радикальных движений и групп, в совершении противоправных, а иногда и преступных действий в связи со своими убеждениями. [6]

К причинам, порождающим экстремистские настроения молодежной среде, необходимо отнести не только социально-экономические противоречия современного общества, но и культурно-воспитательные проблемы: изменение ценностных ориентаций, распад прежних моральных устоев, отсутствие стремления к единению всех народов, проживающих на территории России. Наиболее полно, на наш взгляд, совокупность причин («источников») молодежного экстремизма в России обозначил С.Н. Фридинский [5], добавив к общепринятым следующие социально-политические факторы:

– преобладание досуговых ориентаций над социально полезными;

– кризис школьного и семейного воспитания;

– криминальная среда общения;

– неадекватное восприятие педагогических воздействий;

– отсутствие жизненных планов.

Мусаелян М.Ф. к мерам профилактики экстремизма в целом и в молодежной среде в частности относит следующее:

– прививание подросткам основ толерантности;

– усиление контроля государства за деятельностью общественных и религиозных организаций (благотворительных организаций, военно-патриотических клубов);

– более жесткий контроль за деятельностью СМИ и мониторинг сети Интернет;

– выработка комплексной молодежной политики, а иначе, как отмечает автор, если государство не займется молодежью, ею займутся другие – проповедники (эмиссары, идеологи) ваххабизма, фашизма, национализма [3].

Профилактика киберэкстермизма среди молодежи, на наш взгляд, должна осуществляться одновременно по трем направлениям: юридическому, акмеологическому и технологическому.

В рамках работы по первому направлению предполагается совершенствование законодательства в сфере борьбы с экстремизмом, при этом необходимо учитывать международный опыт в этой области. Киберэкстремисты должны понимать величину ответственности за свои действия и неизбежность наказания. Следует обратить внимание на молодежную политику, а также на законодательство, затрагивающее интересы молодежи. Недовольство судьбой, порожденное отсутствием перспектив, - хорошая почва для внедрения экстремистских идей.

Второе направление связано с работой по формированию системы ценностей молодежи. Только стройная система ценностных ориентиров способна противостоять разрушительному воздействию экстремистских идей. Для этого желательно упростить доступ к объектам культуры, использовать потенциал не только литературы, кино, но и социальных сетей. Интернет-конкурсы, в которых пропагандируются общечеловеческие ценности, интересные онлайн-сообщества – инструментов много, и их можно грамотно задействовать.

В технологическом плане профилактика киберэкстремизма может быть сведена к следующему: фильтрация интернет-контента и персонификация доступа к потенциально опасным ресурсам.

Контент может фильтроваться на трех уровнях: провайдера, сервера и клиентской станции. В случае серверной фильтрации трафик отсеивается на выделенном компьютере, где настроены доступ в Интернет и передача его на остальные компьютеры через локальную сеть. Известные программы для организации серверной контент-фильтрации для Windows – систем: МКФ, UserGate, Kerio, ISA Server, SafeSquid, а также прокси-серверы, на которых можно организовать фильтрацию. Для Linux-систем наиболее популярны DansGuardian и

Mindwebfilter и др. При клиентской фильтрации на каждом компьютере устанавливается и настраивается программа-фильтр, что позволяет задать индивидуальные настройки для каждой машины. Примеры программных продуктов для Windows – систем: Интернет Цензор, ПКФ, NetPolice, KinderGate и др. Для Linux-систем: NetPolice ALT Linux, СКФ и др.(1)

Следует отметить, что зачастую Интернет-фильтры не могут работать с контекстом, поэтому необходимо использовать существующие средства контекстной фильтрации. В настоящий момент она активно используется антиспам-фильтрами, а разработка её методов - перспективное направление научных исследований в России и за рубежом.

Таким образом, профилактика киберэкстремизма – комплексная проблема, для решения которой необходимо задействовать юридические, психолого-педагогические и ИКТ-инструменты. Только их сочетание способно принести желаемый эффект в масштабах государства.

Публикация выполнена в рамках работы над проектом РГНФ № 13-06-00156 «Подготовка педагогических кадров к профилактике и противодействию идеологии киберэкстремизма среди молодежи».

Библиографический список

1. Гаврилова, И.В. Настройка контент-фильтрации в образовательных учреждениях // И.В. Гаврилова, Д.О. Гаврилов. - Новые информационные технологии в образовании: материалы междунар. науч. – практ. конф., Екатеринбург, 12-15 марта 2013 г. ФГАОУ ВПО «Рос. гос. проф. – пед. ун – т». Екатеринбург, 2013. – 390 с.

2. Манхейм К. Диагноз нашего времени. – М., 1994. – С. 445–446.

3. Мусаелян М.Ф. Профилактика экстремизма – важнейшее направление противодействия экстремизму в Российской Федерации // Адвокат. – 2009. – №7. – С.99.

4. Тамаев. РС. Уголовно-правовое и криминологическое обеспечение противодействия экстремизму: монография. – М.: ЮНИТИ-ДАНА: Закон и право, 2012.

5. Фридинский С.Н. Молодежный экстремизм как особо опасная форма проявления экстремистской деятельности // Юридический мир. 2008. – №6. – С. 24.

6. Щербакова. Л.М. Мониторинг экстремизма на территории Ставропольского края / Л. М. Щербакова, П. В. Волосюк. // Вестник Ставропольского государственного университета. – 2011. – № 72 – С. 242 – 247.

Ефимова И.Ю.
к. п. н., доц. каф. прикладной информатики

МЕТОДИКА ОБУЧЕНИЯ РОДИТЕЛЕЙ КОНТРОЛЮ ЗА БЕЗОПАСНЫМ ПОВЕДЕНИЕМ ПОДРОСТКОВ В СЕТИ ИНТЕРНЕТ

ФГБОУ ВПО «Магнитогорский государственный университет», inform@masu-inform.ru

Аннотация

В статье описан опыт решения проблемы обучения родителей контролю за поведением и обеспечению безопасности подростков в сети Интернет с помощью проектной методики на основе андрогогического подхода.

Наш век называют веком цифровых технологий, и действительно, трудно представить себе современную жизнь без компьютеров. А поэтому нет ничего удивительного в том, что дети начинают работать с компьютером очень рано. Тем более компьютеры в качестве источника знаний способны существенно облегчить и улучшить процесс обучения. Но особую полезность представляет собой Интернет. Эта информационная среда обладает огромным потенциалом и способна дать ребенку множество полезных данных. Но в глобальной сети часто встречаются такие ресурсы, показывать которые детям нельзя. Между тем единственным ограничением на них является предупреждением о том, что просмотр содержимого разрешен только людям, достигшим 18-летнего возраста. Естественно, простая надпись не может никого остановить.

Существует классификация нежелательного контента для детей в Интернет от которого следует оберегать детей (порнография и эротика; провокация ненависти; пропаганда насилия; освещение совершения преступлений (особенно в положительном контексте); пропаганда наркотиков; реклама азартных игр) [1].

Актуальность проблемы родительского контроля очень велика. Родители или не контролируют детей в сети Интернет или очень сильно уберегают от «всемирной паутины». Одна из причин недостаточности родительского контроля – низкий уровень знаний самих взрослых о возможностях технического контроля, нежелание разбираться в установке специализированного ПО. При этом растущие требования от родителей - это блокирование посещения детьми сайтов с порнографическим содержанием и доступа к агрессивному, нежелательному для детей контенту. Это является одной из проблем, которую вынуждены решать родители, – доступ ребенка к компьютеру и интернету [1]. Сколько времени ребенок может проводить перед экраном монитора? Как долго ему позволено играть в игры? Как сделать времяпровождение маленького пользователя в сети Интернет безопасным? Необходимо чтобы родители знали ответы на эти вопросы.

Изучив научную литературу и проведя социологический опрос среди родителей, нами было выявлено, что большая часть опрошенных родителей выдвигают требования блокировки нежелательных Интернет-ресурсов для посещения детьми, но ведь этого мало. А все потому что, у самих взрослых низкий уровень знаний об опасностях, которые подстерегают подростков в сети Интернет, о возможностях технического контроля, и самое главное их нежелание разбираться в установке специализированного ПО, которое позволяет обеспечить защиту ребенка [3].

Опасности, которые подстерегают детей при незащищенном доступе в Интернет:

– Высокий риск столкнуться с материалами порнографического, экстремистского, агрессивного содержания.

– Бесконтрольная загрузка различных файлов, которая увеличивает нагрузку на канал оператора связи, а также во много раз увеличивает вероятность заражения компьютера вредоносными программами, что может привести к неблагоприятным последствиям (например, увеличению количества спама, заражению других компьютеров сети и т.п.).

– Бесполезная и, часто, опасная, трата свободного времени на социальные сети, программы мгновенного обмена сообщениями и другие online – сервисы [1].

Проблема обеспечения безопасного и контролируемого доступа детей к интернет - ресурсам беспокоит миллионы родителей, чьи дети имеют возможность выхода во Всемирную сеть. В России насчитывается около 8 млн. пользователей интернета в возрасте до 14 лет, 25% дошкольников пользуются сетью самостоятельно, без надзора родителей. С 10 до 14 лет показатель контактов с нежелательным содержимым сайтов возрастает более чем в 2 раза. Порно сайты просматривают 32% Интернет - аудитории детей до 14 лет. С сайтами об азартных играх, ресурсами о насилии, алкоголе и наркотиках сталкиваются от 13 до 15% ребят, 54% детей оказались защищёнными от нежелательной информации в сети. Это на 12,5% больше, чем полгода назад. Количество домашних пользователей в РФ растёт с увеличением частного компьютерного парка и распространением широкополосного доступа. В том числе растёт количество детей, пользующихся интернетом – не только школьников, но и детей помладше. Кроме того, юные пользователи сети могут выходить в сеть из дома, от друзей или знакомых.

Согласно онлайн-опросу, в 2012 году, RU метрики [1], около половины родителей контролируют Интернет - передвижения своих детей до 10 лет. Контроль над 10-14-летними Интернет - пользователями ослабевает – только 5-10% подростков выходят онлайн под родительским контролем. Сравнивая данные октября с показателями по-

добного исследования в апреле, получается, что контроль за 8 -12 летними детьми вырос на треть. Внимание родителей к Интернет-активности 13-14-летних по-прежнему слишком мало: если из числа дошкольников самостоятельно выходят онлайн порядка 25% ребят, среди восьмилеток этот показатель достигает 37,5%, то 14-летних без надзора родителей в сети порядка 87%. В ходе онлайн-опроса RU метрики [1] было выявлено, сколько детей до 14 лет просматривают «нехорошие» сайты и с какими именно нежелательным содержанием им доводилось сталкиваться. Больше других сайты с нежелательным содержанием просматривают старшие ребята. Почти половина контактов с ненадлежащим наполнением сети приходится порно сайты. Если отмечать какие-либо тенденции контакта несовершеннолетних с содержимым сети нежелательного содержания, то выявляется любопытный факт: 5 – 6 - летние несколько активнее первоклашек, однако уже 8-летки «навёрстывают упущенное». Это, скорее всего, связано с тем, что 7-летние дети начинают пользоваться интернетом именно в школе, где защита от нежелательного контента находиться на довольно хорошем уровне. С 12 до 14 лет показатель контактов с сайтами с нежелательным содержимым возрастает более чем в 2 раза. Заметно увеличивается число посещений сайтов об экстремизме, национализме и насилии. Пик «переходного возраста», который обычно приходится на 14 лет, как раз и демонстрирует, что контактов с нежелательным содержимым сети у пользователей веба в этом возрасте заметно возрастает. Как показано выше, у юных пользователей сети из числа ресурсов с нежелательным содержанием традиционно лидируют порно - сайты – их просматривает приблизительно треть Интернет - аудитории до 14 лет. Вполовину меньше детей интересуются азартными играми (15%), ресурсами о насилии (14%), алкоголе и наркотиках (13%). 54% детей оказались защищёнными от нежелательной информации в сети. Это на 12,5% больше, чем полгода назад. При этом незначительно уменьшилась доля тех, кто просматривает сайты об азартных играх, алкоголе и наркотиках, но заметно снизилась доля ограждённых от порно сайтов, насилия и экстремистские – националистических ресурсов.

В качестве ограничителей активности несовершеннолетних пользователей лидируют три подхода: контроль взрослых (75%), специальные программы, настройки браузеров (30%) и отельная детская учётная запись в операционной системе (15%). Родительский контроль доказывает свою эффективность преимущественно потому, что второй и третий способы, в том числе подозревают самостоятельный веб - серфинг несовершеннолетних пользователей.

Таким образом, сегодня с большой уверенностью можно утверждать, что интенсивное развитие Интернета приводит к возникновению новых видов нежелательной информации. Не все взрослые могут

различить нежелательную информацию от полезной, и вследствие не смогут оградить своих детей. Данная проблема должна решаться в каждой семье в отдельности, так и в целом обществе [5]. Итак, следует понимать, что подключаясь к сети Интернет, ваш ребенок встречается с целым рядом угроз, о которых он может даже и не подозревать. Объяснить ему это обязаны родители перед тем, как разрешить ему выход в Интернет.

Рассмотрим методы борьбы с Интернет - угрозами:

Тщательная фильтрация адресов. Программы родительского контроля позволяют, помимо всего прочего, настроить фильтр для посещения веб-сайтов. С помощью этой функции можно блокировать доступ детей к веб-сайтам, ориентированным на взрослую аудиторию. Регулярно обновляемые «черные списки» содержат адреса определенной категории, и родители могут по своему выбору запретить доступ к тем или иным категориям сайтов.

Другой подход заключается в настройке «белых списков», то есть перечня веб-сайтов, которые разрешено просматривать детям, с запретом доступа ко всем остальным веб-сайтам. Однако такой подход может установить излишне строгие ограничения на использование Интернета. Важно помнить: предусмотренные в программах «черные списки» быстро устаревают, так как каждый день появляются десятки новых веб-сайтов. Для эффективной работы этой функции необходимо регулярное обновление данных списков. Все веб-сайты, которые могут быть пропущены при фильтрации по интернет - адресам, можно отсеять с помощью фильтрации по ключевым словам. В программе задан набор слов, которые неприемлемы для детей. Доступ к веб-сайтам, содержащим такие слова, блокируется. В дополнение к этому родители могут создать собственный список запрещенных веб-сайтов [28].

Безопасное общение

Средства родительского контроля позволяют справиться и с проблемой сохранения личной информации. Они проверяют информацию, вводимую пользователем и отправляемую с компьютера, на наличие таких конфиденциальных сведений, как настоящая фамилия, адрес, номер телефона и название школы, в которой учится ребенок.

Входящие в состав продукта Norton Internet Security функции родительского контроля и управления конфиденциальностью поддерживают фильтрацию веб-сайтов по URL-адресам и ключевым словам, а также предотвращают отправку конфиденциальной информации. Эту функцию можно применять не только при общении с другими пользователями через Интернет, но и при покупке товаров в Интернет-магазинах, для того чтобы ребенок не указывал адрес и номер банковской карты на веб-сайтах электронной коммерции [7].

Контроль за продолжительностью работы в Интернете

Работа в Интернете опасна не только тем, что можно натолкнуться на веб-сайты с недопустимым содержимым или сайты злоумышленников. Родителей также волнует то, сколько времени ребенок проводит в Интернете и хватает ли у него времени на уроки и другие увлечения. Средства родительского контроля позволяют ограничить время работы ребенка в Интернете [7].

Веб-браузеры, предназначенные специально для детей

В некоторых веб-браузерах предусмотрены правила, запрещающие детям доступ к веб-сайтам, содержимое которых для них не предназначено. Такие веб-браузеры можно использовать в качестве дополнительной меры защиты для маленьких детей, однако они не подходят для подростков, так как содержат слишком короткий «белый список» веб-сайтов. Кроме того, те подростки, которые хорошо умеют работать с компьютером, смогут отключить эту защиту.

Дополнительные функции

Некоторые средства родительского контроля поставляются в комплекте с другими функциями, такими как антивирусная защита или брандмауэр. Например, продукт Norton Internet Security представляет собой комплексное решение, включающее в себя антивирусную защиту, брандмауэр, средства родительского контроля, средства управления конфиденциальностью и функцию защиты от спама [7].

Однако установкой программных средств нельзя решить все проблемы. Даже при наличии средств родительского контроля следует принять следующие меры предосторожности:

1. Установите компьютер в общей комнате, особенно если у вас есть дети младше 15 лет. В этом случае ребенок не будет находиться наедине с компьютером.
2. Помогите ребенку сделать первые шаги в сети Интернет и расскажите о тех опасностях, с которыми можно там столкнуться.
3. Составьте свод правил хорошего поведения. Internet - это прекрасная возможность для общения, обучения и отдыха. Но следует понимать, что, как и реальный мир, Всемирная Паутина может быть весьма опасна.

Изначально Интернет развивался вне какого-либо контроля, поэтому сейчас он представляет собой огромную базу информации, причем далеко не всегда безобидной. В последнее время количество детей и подростков, получающих возможность выходить в Интернет, существенно увеличивается, а их возраст уменьшается. И это значит, что проблема обеспечения безопасности наших детей становится все более острой. Помочь могут только родители. Лучший способ обеспечить безопасное использование Интернет – иметь доверительные и доброжелательные отношения с детьми. Однако следует понимать, что одно только воспитание без организации контроля практически бесполезное

занятие. Равно как и наоборот. Только объединив эти средства, можно помочь своим детям чувствовать себя в безопасности и оградите их от влияния злоумышленников в Интернет [8].

Проблема контроля ребенка подроста очень велика. Существует очень много угроз, но при этом существует множество решений по этому вопросу. Главное, чтобы сам родитель знал ответ на существующую проблему. Для информирования родителей созданы два проекта на http://letopisi.ru/- «Родительский контроль: Интернет территория безопасности» и «Осторожно паутина под напряжением». Эти проекты дадут более четкое представление о существующих проблемах в сети Интернет.

С помощью проектной методики с использованием андрогогического подхода разработана систему заданий для обучения родителей в рамках проекта: «Родительский контроль: Интернет территория безопасности», как мы считаем, этот метод поможет наилучшим способом углубить родителей в столь сложную тему. Эта программа обучения идет с компьютерной поддержкой.

Была выбрана платформа для реализации проекта – letopisi.ru [9]. Это означает, что сами родители не будут создавать проекты на определенные темы, они будут опираться на проект, созданный учителем. Но при этом, именно родители будут выполнять всю ту работу, которая включена в состав проекта.

Материал рекомендуется изучать в течение 6 семинаров (продолжительность одного семинара 1 час 30 минут), т. е. около 9 часов, в это время входят семинары и работа дома.

Целевая аудитория: родители подростков.

Тип проекта:

1 По предметно-содержательной области – меж предметный;
2 По характеру координации – с явной координацией;
3 По характеру контактов – внешний;
4 По количеству участников – индивидуальный или групповой;
5 По продолжительности выполнения – долгосрочный.

Предметы, с которыми связан данный проект:

1. Информатика;
2. Педагогика

Задачи семинара:

1. Ознакомление родителей с проблемой информационной безопасности;
2. Ознакомление с программами родительского контроля;
3. Развитие навыков работы со своими детьми;
4. Описание родителями своего видения современной проблемы;

5. Развитие познавательного интереса, творческой активности, умения излагать мысли;
6. Совершенствование мыслительных приемов анализа и синтеза;
7. Воспитание негативного отношения к нежелательному контенту у родителей и их детей;

Техническое обеспечение, необходимое для успешного осуществления работы: компьютеры, подключенные к Интернету.

План работы над проектом:

- Информационный этап: рассказ родителям о создании проектов, опыте применения проектов в этой области, описание эмоций и ощущений при работе над проектом;
- Формулировка задач, функций каждого родителя: учитывается ситуация каждого родителя в данной проблеме;
- Подготовка проекта: проект готовит учитель. Учителю нужно знать, как продвигается работа по изучению проекта, так как проект – один из лучших, возможных способов решения проблемы;
- Коррекция: учитель советует родителям, что нужно сделать, какие дополнения внести, чтобы проект стал интересным, исправляет ошибки;
- Анализ представленных проектов: спрашивается мнение каждого ребенка о проекте, что понравилось, какие изменения необходимо внести, чтобы следующий проект стал более удачным. Заключительное слово предоставляется учителю. Важно найти теплые слова благодарности всем детям и родителям за выполненную работу.

Этапы проекта

В «Таблице 4» изложена общая последовательность этапов работы над проектом и раскрыта их сущность. На усмотрение учителя некоторые этапы могут объединяться, поэтому может меняться содержание работы на данных этапах.

Конспект семинаров

Семинар № 1:

Этап 1: Эссе «Родительский контроль: Интернет территория безопасности».

Нужен для того, чтобы посмотреть насколько родители понимают, что такое Интернет, родительский контроль. Выявить начальные знания обучающихся. После пройденных семинаров они будут снова писать эссе на эту тему, и тогда можно сказать, на сколько родители поняли эту проблему, чтобы в следующем семинаре уже усовершенствовать задания для семинара «Родительский контроль: Интернет территория безопасности »

На данном этапе родителям необходимо зайти на сайт http://letopisi.ru/, затем найти учебный проект «Родительский контроль: Интернет территория безопасности». Ознакомиться с ним. (http://letopisi.ru/index.php/Учебный_проект_Родительский_контроль:_Интернет_территория_безопасности).

На первом этапе, предлагается написать эссе на тему «Родительский контроль: Интернет территория безопасности». Изложить свое видение проблемы на данный момент, возможно используя свой опыт, либо опыт знакомых. Раскрыть такие понятия как родительский контроль, Интернет, а также описать, в чем заключается родительский контроль, и возможные способы борьбы с нежелательной информацией в Интернете.

Этап 2: Введение в тему: «Родительский контроль: Интернет территория безопасности».

Введение представлено родителям в виде презентации, ознакомиться с которой можно перейдя по ссылке:

http://letopisi.ru/index.php/Учебный_проект_Родительский_контроль:_Интернет_территория_безопасности

и далее нажав гиперссылку «презентация «Введение»». Она содержит ответы на такие вопросы как чем опасен Интернет для детей, какие встречаются угрозы наиболее часто, а также статистику, методы борьбы с угрозами и меры предосторожности.

Этап 3: Рефлексия.

Целью на этой стадии проекта является посмотреть на сложности, которые были при выполнении заданий, родители должны проанализировать свою работу. Анализ родителями пройденного материала, который осуществляется на сайте http://letopisi.ru/.

Семинар № 2:

Этап 1: Круглый стол на тему: «Нужны ли программы контроля?».

План:

1. Что такое программы контроля в Интернет? Зачем они нужны?
2. Какие есть программы контроля? Какая программа контроля на ваш взляд лучше защитит вашего ребенка?
3. Вывод. Нужны ли программы контроля?

Целью данного этапа является рассмотрение со всех сторон плюсов и минусов программ, сделать вывод нужны ли они вообще. Просмотреть есть ли компьютерная зависимость у ребёнка, чтобы потом предпринять меры об улучшении результата.

Этап 2: Заполнение анкеты по девиантному поведению, позволяющую выявить компьютерную зависимость у ребенка, выводы (домашняя работа).

В учебном проекте на сайте http://letopisi.ru/ перейдя по ссылке анкета, родителям необходимо пройти ее во время домашней работы. С помощью анкеты следует посмотреть, есть ли компьютерная зависимость у ребёнка, чтобы потом предпринять меры. Таким образом проанализировать, есть ли зависимость у ребенка.

Этап 3: Рефлексия.

Родителям необходимо проанализировать изученный материал, и описать свои ощущения о проделанной работе.

Семинар № 3:

Этап 1: Обзор программ родительского контроля.

Будет проходить в виде лекции, сопровождающейся презентацией. Для того чтобы просмотреть презентацию с обзором программ, необходимо перейти по ссылке презентация «Обзор программ родительского контроля», в которой описаны следующие программы родительского контроля:

- Родительский контроль в Windows Vista;
- КиберМама;
- KidsControl 1.6;
- Time Boss 2.34;

Этап 2: Лабораторная работа «Программа родительского контроля Time Boss»

Time Boss создан, чтобы дать родителям возможность ограничить время, которое наши дети проводят, играя в компьютерные игры или сидя в интернете.

Задание 1

Русифицировать программу. Программа полностью на английском языке, нужно перевести на русский.

Задание 2

Настроить следующие параметры работы в Интернет:

– максимальное время работы: не более 5 часов в день;
– время работы в интернете: пн.-пт. 14-21, сб.-вс. 10-17;
– время непрерывной работы: 1 час, перерыв 15 минут;
– в выходные установлен дополнительный час и снято ограничение непрерывной работы.

При завершении времени, выделенного на работу в Интернет, предупредить пользователя сообщением «Ваше время истекло, через 5 минут Интернет будет заблокирован».

Задание 3

Установить следующие настройки для доступа к сайтам:

– интернет-фильтр: максимум;
– настроить доступ к сайту vkontakte.ru (а так же *.vkontakte.ru, vk.com и *.vk.com): доступ в течение дня на 1 час, время доступа пн.-пт. 19-21, сб.-вс. в любое время на 2 часа;

– запретить полный доступ к сайту rutracker.org;

– внести в белый список любой сайт, настроить его по своему усмотрению.

Задание 4

Запретить доступ к играм на вашем компьютере:

– игра №1: полный запрет на запуск;

– игра №2: разрешить запуск ежедневно на 1 час, на выходных без ограничений.

Задание 5

Установить ограничения:

– редактор реестра;

– диспетчер задач;

– установка и удаление программ;

– доступ к диску С;

– доступ к папке, в которой находятся ваши учебные материалы.

Задание 6

Настроить награды:

– Молодец: +30 минут дополнительное время работы на компьютере;

– Умница: +1 час работы в Интернет;

– Гений: +2 часа работы в Интернет и на компьютере.

Задание 7

Установить параметры работы программы:

– пароль;

– хранить данные 15 дней;

– делать скриншот экрана раз в 10 минут, снимки хранить 15 дней;

– настроить программы, которые разрешено использовать в сети Интернет;

– останавливать время при работе скринсейвера.

Данная лабораторная работа разработана Черновой Еленой Владимировной по курсу «Информационная безопасность в системе открытого образования».

Таблица 4. Этапы проекта

Стадия работы над проектом	Продолжительность	Цель на этой стадии проекта	Деятельность родителей	Деятельность учителя
Семинар № 1: Этап 1: Эссе «Родительский контроль: Интернет территория безопасности»	30 минут	Посмотреть насколько родители понимают, что такое Интернет, какие опасности есть в Интернет, как осуществить родительский контроль	Зайти на страничку с проектом. Открыть документ, нажав на ссылку – эссе «Родительский контроль: Интернет территория безопасности».	Объяснить ход работы
Этап 2: Введение в тему: «Родительский контроль: Интернет территория безопасности»	50 минут	Осведомить родителей о том, на какую тему будут проходить семинары, ввести в тему, заинтересовать	Вникнуть в тему и в проблему	Объяснение темы с помощью презентации
Этап 3: Рефлексия	10 минут	Посмотреть на размышление человека, направленное на анализ самого себя (самоанализ)собственных состояний, своих поступков и прошедших событий.	Проанализировать работу, отписаться в блоге	Анализ и доработка заданий.

Семинар № 2: Этап 1: Круглый стол на тему: «Нужны ли программы контроля?»	50 минут	Рассмотреть со всех сторон плюсы и минусы программ, сделать вывод нужны ли они вообще	Подготовка к круглому столу, на основе пройденного семинара.	Направлять родителей на получение положительного результата
Этап 2: Заполнение анкеты по девиантному поведению, позволяющую выявить компьютерную зависимость у ребенка, выводы (домашняя работа)	30 минут	Просмотреть есть ли компьютерная зависимость у ребёнка, чтобы потом предпринять меры	Проанализировать своего ребенка с помощью анкеты	Дать анкету для заполнения
Этап 2: Рефлексия	10 минут	Посмотреть на размышление человека, направленное на анализ самого себя (самоанализ) собственных состояний, своих поступков и прошедших событий	Проанализировать работу, отписаться в блоге	Анализ и доработка заданий.
Семинар № 3: Этап 1: Обзор программ родительского контроля	40 минут	Рассмотреть все виды программ родительского контроля, объяснить все плюсы и минусы этих программ, рассмотреть их ценовую политику	Слушать преподавателя, задавать вопросы	Объяснять тему, раскрыть вопрос.

Этап 2: Лабораторная работа «Программа родительского контроля Time Boss»	40 минут	После рассмотрения программ родительского контроля, и мы разберем работу одной из программ на практике, для того чтобы родители потом не боялись устанавливать её дома	Выполнение лабораторной работы	Смотреть за правильностью выполнения, подсказывать.
Этап 3: Рефлексия	10 минут	Посмотреть на размышление человека, направленное на анализ самого себя (самоанализ) — собственных состояний, своих поступков и прошедших событий.	Проанализировать работу, отписаться в блоге.	Анализ и доработка заданий.
Семинар № 4: Этап 1: Круглый стол, посвященный домашней работе	50 минут	Узнать, насколько непонятен Интернет ребенку и есть ли у него «Интернет зависимость»	Провести анализ результатов, принятие решений ситуаций	Помочь подобрать метод борьбы со сложившейся ситуацией
Этап 2: Эссе «Родительский контроль: Интернет территория безопасности», на основе приобретенных знаний	30 минут	Проверка усвоения материала данного на семинарах	Зайти на страничку с проектом - Открыть документ, нажав на ссылку – эссе «Родительский контроль: Интернет территория безопасности»	Наблюдение

Этап 3: Рефлексия	10 минут	Посмотреть на размышление человека, направленное на анализ самого себя (самоанализ) — собственных состояний, своих поступков и прошедших событий	Проанализировать работу, отписаться в блоге	Анализ и доработка заданий.
Семинар № 5: Этап 1: Круглый стол для подведения результатов.	1 час 10 минут	Закрепление результатов, выявление сложностей при прохождении заданий проекта	Анализ семинаров за круглым столом	Анализ усвоенного материала.
Этап 2: Рефлексия	20 минут	Посмотреть на размышление человека, направленное на анализ самого себя (самоанализ) — собственных состояний, своих поступков и прошедших событий	Проанализировать работу, отписаться в блоге	Анализ и доработка заданий.

Этап 3: Рефлексия.

Деятельность родителей на данном этапе заключается в том, чтобы проанализировать изученный материал и описать свою работу.

Семинар № 4:

Этап 1: Круглый стол «Результаты домашней работы».

Целью круглого стола является получение информации от родителей на сколько запущена ситуация у ребенка с помощью анкеты. Ведется обсуждение волнующих моментов. Родителям необходимо проанализировать ситуацию, а учителю помочь подобрать метод борьбы со сложившейся ситуацией.

Этап 2: Эссе «Родительский контроль: Интернет территория безопасности»

Данный этап заключается в том, чтобы родители написали эссе на тему «Родительский контроль: Интернет территория безопасности» основываясь на приобретенных знаниях после пройденных семинаров.

Этап 3: Рефлексия.

После проделанной работы родителям необходимо проанализировать свою работу.

Семинар № 5:

Этап 1: Круглый стол для подведения результатов.

Родителям необходимо проанализировать проделанную работу и представить ее в обсуждении на круглом столе. Производится закрепление результатов, возможно выявление каких - либо сложностей, возникших при выполнении проекта. Учителю необходимо проанализировать усвоенный родителями материал.

Этап 2: Рефлексия.

После проделанной работы родителям необходимо проанализировать свою работу.

Семинар № 6:

Данный семинар называется «Осторожно паутина под напряжением», представляет собой проект, предназначенный для детей 10-12 лет и должен проводиться при обоюдном согласии родителей и учителя в качестве консультанта инструктора.

Этап 1: Вводная презентация.

Расположена на сайте http://letopisi.ru/. Данная презентация представляется учителем и содержит в себе основные понятия по данной теме.

Этап 2: Тест

Тест проводится учителем, перейти к которому можно по ссылке «тест», для того, чтобы проверить уровень знаний учащихся по данной теме.

Этап 3: Разделение на подгруппы.

Ученикам необходимо разделиться на 2 подгруппы, для того,

чтобы раскрывать проблемные вопросы. Первой группе необходимо создать презентацию, а второй - буклет.

Этап 4: Сказка

Сказка представляется во время того, как учащиеся выполняют работу над презентацией и блогом. Это задание является творческим, оно представлено на сайте http://letopisi.ru/ , по ссылке «сказка».

Этап 5: Круглый стол

Круглый стол проводится после того как, учащиеся закончат работу над частями проекта, и описания своих мнений и впечатлений в блоге, который находится на том же сайте.

Этап 6: Тест

Данный тест идентичен тесту, проведенному на этапе 2, проводится с целью выявить у учеников усвоенный материал и полученные знания после прохождения проекта. Производится анализ, и приводятся результаты работы над проектом.

Дидактические цели проекта:

1.Сформировать у родителей представление о сети Интернет;

2.Сформировать у родителей знания об угрозах Интернет;

3.Сформировать у родителей навыки работы с компьютером, борьбы с Интернет угрозами;

4.Как осуществлять контроль за подростками в сети.

В дополнении к курсу семинаров родителям предлагается учебное пособие в виде проекта «Осторожно паутина под напряжением» . По желанию учителя и родителей может пройти еще один семинар (семинар № 6), который поможет родителям лучше объяснить детям, что такое Интернет и все подводные камни сети.

Краткое содержание проекта «Осторожно паутина под напряжением»: прежде всего, рассматривается информация о том, как в наше время можно защититься в сети Интернет, а также как можно распознать угрозы и мошенничество, а так же как нужно себя вести в паутине: правила, авторское право и этикет.

Дидактические цели / Ожидаемые результаты обучения:

После завершения проекта дети узнают о том, какие подводные камни есть в океане информации и как избежать столкновения с ними.

Знания:

– этикета в Интернете;

– авторского права в Интернете;

– как защищать компьютер при работе в Интернете;

– как защищать себя при работе в Интернете.

Умения: оберегать себя и компьютер от угроз сети.

Навыки:

– компьютерная грамотность;

– безопасное использование Интернета;

– использование программ контроля.

До работы над проектом проводится оценка начальных (базовых) знаний детей: теоретические знания о том, что такое компьютер и Интернет.

Во время выполнения самостоятельных заданий, дети объясняют ход их выполнения, показывая тем самым уровень усвоения пройденного материала.

После завершения работы над проектом:

– в конце каждого занятия проводится дискуссия с ребёнком для выявления уровня усвоения материала с целью стимулирования их дальнейшего интереса к изучению предмета дискуссии.

Таким образом, с использованием проектной методики разработанная система заданий для обучения родителей в виде серии семинаров на тему: «Родительский контроль: Интернет территория безопасности», будет наилучшим образом способствовать углублению родителей в столь сложную тему.

Данный проект поможет внедрить в образовательный процесс при обучении бедующих учителей информатики, в работу с родителями. Применение разработанной методики будет способствоватьт повышению эффективности обучения родителей и в области информационной безопасности и может быть рекомендована при обучении родителей детей-подростков.

Публикация выполнена в рамках проекта РГНФ № 11-06-01006 «Разработка и апробация модели подготовки научно-педагогических кадров к обеспечению информационной безопасности в ИКТ-насыщенной среде».

Библиографический список

1. Абулин. К.А. Безопасность в интернете [интернет портал], URL: http://www.comprice.ru/ (дата обращения 18.03.13)

2. Бабанский. Ю.К. Избранные педагогические труды. – М. : Педагогика, 1989. – 560 с.

3. Богданова. И.Ф. Интернет и современное общество: Труды XI Всероссийской объединенной конференции (28–30 октября 2008 г., Санкт-Петербург). – СПб.: Факультет филологии и искусств СПбГУ, 2008. – С. 24–26.

4. Гильбух. Ю.З. Психодиагностическая функция учителя: пути реализации / Психология трудового воспитания школьников. – Киев: Радяньска школа, 1987. – 255с.

5. Детские браузеры - защита ребенка от угроз интернета [интернет портал], URL: http://www.3dnews.ru/software/detskie_brauzeri/ (дата обращения 12.01.11)

6. Змеев. С.И. Андрагогика и образование взрослых: основные понятия и термины. Понятийный аппарат педагогики и образования. – Вып. 2. – Екатеринбург, 2002.
7. Зеркина. Е.В., Чусавитина. Г.Н. Подготовка будущих учителей к превенции девиантного поведения школьников в сфере информационно-коммуникационных технологий : монография. – Магнитогорск: МаГУ, 2008. – 185 с.
8. Программы контроля, родительский контроль [интернет портал], URL: http://nicekit.ru/parental-control/time-boss.php (дата обращения 18.05.2011)
9. Социальный сервис «Летописи» [интернет портал], URL: http://letopisi.ru/ (дата обращения 17.06.12)

Давлеткиреева Л.З.
к.п.н., доц. каф. информационных систем.
Ижбаев С.А.
учитель МОУ «СОШ №20»,
заместитель директора по безопасности

РОЛЬ ГОСУДАРСТВА, БИЗНЕСА, ИНСТИТУТОВ ГРАЖДАНСКОГО ОБЩЕСТВА И СМИ В ФОРМИРОВАНИИ СИСТЕМЫ ПРОТИВОДЕЙСТВИЯ ИДЕОЛОГИИ КИБЕРЭКСТРЕМИЗМА

ФГБОУ ВПО «Магнитогорский государственный университет»,
ldavletkireeva@masu-inform.ru

Аннотация

В статье описана система формирования противодействий идеологии киберэкстремизма. Взаимодействие и зависимости между основными факторами, влияющими на ее формирование: Государство, Бизнес, Общество и СМИ, их влияние и значимость каждой структуры в системе.

Теоретическое и практическое значение исследования системы противодействия кибертерроризму вызвано необходимостью глубокого осмысления теоретико-методологических, организационных, политических основ разработки и реализации данного вида противодействия и определяется следующими обстоятельствами.

Во-первых, одним из главных факторов развития социально-политической системы является производство и использование информации. В современных условиях она играет ключевую роль в жизнедеятельности каждого человека. Компьютеры и информационно-коммуникационные системы, используются во всех сферах деятельности человека и государства в целом. Это обеспечение национальной безопасности, предоставление государственных услуг в

области здравоохранения, образования, ЖКХ, управления аэро- и железнодорожным транспортом, торговли-, финансов, а также межличностного общения и др. Влияние глобальных сетей на социально-политическое развитие общества многогранное противоречиво. С одной стороны, они способствуют развитию потенциала человека через компьютерные игры, обучающие и развлекательные программы, интерактивное телевидение, электронную прессу. Глобальные сети оказывают влияние на электоральное поведение субъектов политики, процесс организации и проведения избирательных кампаний, механизмы коммуницирования власти и общества, презентацию и отстаивание политическими представителями своих интересов. Модифицируя систему взаимоотношений и взаимодействия институтов гражданского общества и государства, глобальные сети способствуют формированию конструктивного диалога между ними. С другой стороны, стремительное развитие информационно-коммуникационной сферы привело к появлению новых видов преступлений - компьютерной преступности и компьютерного терроризма. От деятельности кибертеррористов в виртуальном пространстве могут пострадать тысячи пользователей сетей, не только отдельные люди, но и целые государства. Количество преступлений, совершаемых в киберпространстве, растет пропорционально числу пользователей компьютерных сетей. Современные террористические организации активно используют информационно-коммуникационные технологии, наряду с традиционными средствами, при этом, время перехода от угрозы до реального акта кибертеррористов значительно «уменьшается».

Во-вторых, актуальность исследования этого вида политики возрастает в условиях усложнения социальной структуры и политической жизни общества, что кардинально модифицирует каналы артикуляции, и агрегирования интересов социально-политического взаимодействия создает опасность для формирования кардинально противоположных подходов к оценке политических событий процессов, решению конкретных задач, выбору социальных ориентиров форм политической активности. Опасность деструктивных явлений усиливается в условиях падения уровня легитимности власти, доверия населения к политическим институтам в целом и политике властвующей элиты в частности. Эти и другие явления в какой-то мере инициируют кибертеррористическую деятельность, усиливая потенциал кибертерроризма как способа давления на власть, поскольку они, нередко ведут к неустойчивости функционирования социально-политической системы, несогласованности действий и взаимодействий политических институтов и лиц, функции которых связанны с

разработкой и реализацией политики противодействия этому явлению. Появление нового вида терроризма угрожает безопасности личности, общества и государства на всех уровнях политики, что и обусловливает необходимость его всестороннего изучения.

В-третьих, эффективность политики противодействия кибертерроризму зависит не только от устойчивости функционирования социально-политической системы, развитости контроля государства над процессами в виртуальном пространстве, соблюдения правовых норм в данном сегменте внутренней и внешней политики, развития правовой грамотности элиты и населения и т.д. Во многом она обусловлена наличием у властвующей элиты и представителей специальных служб инструментария познания анализируемого феномена, что невозможно без его концептуального осмысления, расширения и обогащения методологической палитры за счет подходов, позволяющих наиболее полно изучить сущность и особенности нового вида терроризма.

Таким образом, теоретическая и практическая значимость, недостаточная разработанность в мировой и отечественной практике эффективных социально-политических и правовых механизмов противодействия кибертерроризму обусловливает необходимость концептуального осмысления этого феномена, анализа его сущности, особенностей и тенденций функционирования, поиска и обоснования путей минимизации, осмысления роли государства в противодействии этому негативному явлению.

Кибертерроризм - это многогранный феномен, обусловленный во многом бесконтрольным использованием глобальных сетей, недостаточным вниманием со стороны государства, гражданского общества и спецслужб к данному сегменту политики, проявляющийся в атаках на компьютеры, компьютерные программы и сети или находящуюся в них информацию, с целью создания атмосферы страха и безысходности в обществе во имя достижения целей и интересов субъектов террористической деятельности, требующий объединения усилий мирового сообщества для эффективного противодействия ему.

Проблема обеспечения безопасности компьютерной информации и технологий является сегодня одной из самых острых для большинства стран мира. В первую очередь это касается использования информационных систем и сетей в государственном управлении, военной и промышленной, сферах, бизнесе. Разработка эффективной политики противодействия кибертерроризму ведется по следующим основным направлениям: определение приоритетных целей (глобальные, региональные, национальные) и средств (ресурсов), выявление возможных кибертеррористических угроз, защита населения, создание и координация I международной

инфраструктуры, противодействия кибератакам, включающей в себя разработку специальных антитеррористических программ, норм международного права и др.

Обеспечение безопасности от кибертеррористической угрозы становится одним из главных приоритетов национальной безопасности России. Государство осуществляет политику противодействия кибертерроризму в рамках реализации основных принципов построения информационного общества. Это обусловлено необходимостью создания общенациональных систем безопасности информационно-коммуникационной инфраструктуры, обеспечивающих надежную ее защиту от возможных угроз.

В противодействии кибертерроризму приоритетное значение должно принадлежать оперативному пресечению ибертеррористических атак на стадии их подготовки (анализ информации, разработка законов, контроль со стороны государства), а так же проведению на постоянной основе мониторинга состояния информационно-коммуникационного пространства, донесению необходимой информации до населения, профилактической работе (воспитательная, правовая, организационная) и др. Перечисленные меры должны всегда находиться в центре внимания федеральной и региональной власти. Пролонгация кибертеррористических атак в повседневную жизнедеятельность социума обусловила необходимость, разработки различных программ и мероприятий по организации разнообразной помощи жителям, пострадавшим от кибертеррористических действий, минимизации наносимого ущерба.

Механизмы политического регулирования в сфере государственной политики противодействия кибертерроризму предполагают учет таких факторов, как наличие у власти экономических, технических, правовых, организационных и иных ресурсов; которые необходимо задействовать в процессе реализации антитеррористических акций и программ, уровень, ответственности граждан, характер освещения данной проблемы в СМИ, последствий совершения кибератак, уровень использования других компьютерных сетей, анализ сайтов, состояние систем защиты собственных сетей, а так же объектов повышенной опасности.

В 2008 и 2011 гг. было проведено исследование, целью которого было выявить мнение населения (студенты ВУЗов, и специалисты ИТ) об эффективности государственной политики противодействия кибертерроризму. Было опрошено 800 человек. Исследование показало низкую информированность респондентов об исследуемом явлении, наличие не полной и не всегда достоверной информации о данном явлении необходимость институционализации профилактической-

работы государства и спецслужб в качестве ведущего направления политики противодействия этому явлению.

Анализ влияния государства, бизнеса, институтов гражданского общества и СМИ в сфере формирования системы противодействия идеологии киберэкстремизма приводит нас к выводу: каждая из вышеперечисленных сфер деятельности человека в равной степени влияют на формирование данной системы противодействия. Вместе с тем и система противодействия непосредственно влияет на веяние киберэкстремизма, что приводит к общему заключению: мобилизуя и преобразовывая систему противодействия экстремизму необходимо основываться на всех аспектах формирования, каждая сфера деятельности человека и государства в той или иной степени подвержена кибератакам, предотвращение которых предполагает предусмотрение каждого аспекта в частности и во всех взаимосвязях системы.

Разработка проекта выполнена при поддержке гранта РГНФ № 13-06-00156 «Подготовка педагогических кадров к профилактике и противодействию идеологии киберэкстремизма среди молодежи».

Библиографический список

1. Рекомендации по противодействию экстремистским проявлениям в среде обучающихся в образовательных учреждениях – [Электронный ресурс] – Режим доступа: http://mardasova-nadezhda.narod.ru/index/0-21
2. Терроризм – [Электронный ресурс] – Режим доступа: http://bibliofond.ru/view.aspx?id=493315
3. Упорников Р.В. Политико-правовые технологии противодействия информационному экстремизму в России: автореф. дис. канд. юрид. наук. Ростов н/Д., 2007.
4. Паин Э.А. Социальная природа экстремизма и терроризма //Общественные науки и современность. 2002. № 4. С.115
5. Кубякин Е.О. Молодежный экстремизм в условиях становления глобального информационного общества. Краснодар, 2011.
6. Основные виды и формы экстремизма – [Электронный ресурс] – Режим доступа: http://www.ekstremizm.ru/biblioteka/knigi/item/217-vidy-i-formy-ekstremizma

Истомина В.Ю.
начальник Отдела по обеспечению реализации ГОС
Назарова О.Б.
к.п.н, доц. каф.информационных систем

ФОРМЫ И МЕТОДЫ ПРОФИЛАКТИКИ И ПРОТИВОДЕЙСТВИЯ КИБЕРЭКСТРЕМИЗМУ И КИБЕРТЕРРОРИЗМУ В ОБРАЗОВАТЕЛЬНОЙ СИСТЕМЕ

Управление образования Курчатовского р.-на Администрации
г. Челябинска, veraistomina@mail.ru
ФГБОУ ВПО «Магнитогорский государственный университет»,
abiturient@masu.ru

Аннотация

В данной статье рассматриваются причины и последствия такой формы социальной девиации как кибертерроризм, его влияние на социальную среду молодежи, способы противодействия данному явлению в системе общего образования.

Мы живем в век бурного технического прогресса, современных стремительно развивающихся и постоянно обновляемых высоких технологий, информационно-компьютерных систем. Компьютеры и телекоммуникационные системы используются во всех сферах жизнедеятельности - от решения проблем национальной безопасности, здравоохранения и управления транспортом до торговли, финансов, образования и просто межличностного общения. Информатизация развивается стремительно и ведёт к созданию единого информационного пространства, в рамках которого производится накопление, обработка, хранение и обмен информацией между субъектами этого пространства - людьми, организациями, государствами.

Информационный век принес миру не только повсеместное развитие технологий и компьютеризацию всей жизни, но и привел к появлению такой формы социальной девиации как кибепреступность, которая в настоящее время получает все более широкое развитие.

Взломы банковских электронных сетей, пропагандистские войны, экстремизм в Интернете, атаки на правительственные сайты – вот далеко не полный перечень того, чем порой оборачивается для государств и отдельных людей информационная эра.

Кибертерроризм является новой формой терроризма, которая для достижения своих террористических целей использует современные информационные технологии. По своему механизму, способам совершения и сокрытия такие преступления характеризуются высоким уровнем латентности, низким уровнем раскрываемости и наносят несравнимо больший вред, нежели преступления «в реальном мире», поскольку своей целью имеют повреждение и вывод из строя важней-

ших объектов инфраструктуры, информационный шантаж и совершаются удаленно.

По словам профессора Джорджтаунского университета Дороти Деннинг, ведущего специалиста в области киберпреступности: «…кибертерроризм является продуктом слияния терроризма и киберпространства»[1]. Как правило, под этим понимается «использование информационных технологий для организации осуществления атак против сетей, компьютерных систем и телекоммуникационной инфраструктуры, а также для обмена информацией между террористами в электронном виде [2].

К этому виду терроризма относятся: взлом компьютерных систем инфраструктурных объектов (водоснабжение, канализация, лифт, светофоры), внедрение вирусов в правительственные сети, преднамеренная подрывная деятельность, либо применение насилия с использованием компьютеров и/или сети Интернет с намерением причинить вред социальным, идеологическим, религиозным, политическим ценностям общества. Последнее особенно важно, т.к. наличие религиозной, идеологической или политической подоплеки помогает отличить кибертерроризм от обыкновенной компьютерной преступности (т.е. кражи информации, рассылки компьютерных вирусов и т.д.).

Обнаружить и нейтрализовать виртуального террориста весьма сложно из-за слишком малого количества оставляемых им следов, в отличие от реального мира, где, можно предположить, следов содеянного остается все же больше.

Кибертерроризм – это серьезная угроза человечеству. Опыт, который уже имеется у мирового сообщества в этой области предположительно свидетельствует о несомненной уязвимости любого государства, тем более, что кибертерроризм не имеет государственных границ, кибертеррорист способен в равной степени угрожать информационным системам, расположенным практически в любой точке земного шара. [3]

В докладе ООН «Использование интернета для террористических целей» социальные сети: Facebook, Twitter и YouTube рассматриваются как место вербовки сторонников террористических организаций. Известны факты использования социальных сетей с террористическими целями и в России.

В Красноярский суд было передано дело 20-летнего парня, который создал в социальных сетях группу, сочувствующую террористам. В нее записались около 800 уроженцев Северного Кавказа. На своей личной страничке подсудимый выложил три видеоролика, которые объясняли и оправдывали террор. "Данный факт был выявлен сотрудниками УФСБ России по Красноярскому краю. Уголовное дело было заведено по части 1 статьи 282 УК РФ (возбуждение ненависти

либо вражды), хотя в российском законодательстве для такого рода дел есть и особая статья - 205.2 УК РФ "публичное оправдание терроризма". Именно по ней в Ростовской области осудили 19-летнюю жительницу Аксая. Девушка два года публиковала на своей электронной страничке "В Контакте" статьи и картинки, которые оправдывали экстремистские или террористические действия. Ростовская студентка публиковала именно такие картинки вовсе не случайно. Она еще и собирала средства для поддержки осужденных террористов и их семей. Для этого и нужно было вызвать сочувствие к преступникам. Таким образом, ее благотворительная деятельность оказалась вне закона.

Размещение в сети Интернет публикаций экстремистского характера закончилось для 16-летнего подростка обвинительным заключением по части первой статьи 282 (возбуждение ненависти либо вражды по признаку национальности, совершенное публично или с использованием средств массовой информации), части первой статьи 280 (публичные призывы к осуществлению экстремистской деятельности) Уголовного кодекса Российской Федерации.

Следственными органами было установлено, что под влиянием московских событий, развернувшихся на межнациональной почве, обвиняемый с домашнего компьютера разместил «В контакте» текст экстремистского содержания с высказываниями, побуждающими к враждебным действиям против части населения страны и города Челябинска по национальному признаку. Санкция статьи за наиболее тяжкое преступление предусматривает в качестве наказания лишение свободы на срок до трех лет. После утверждения прокурором обвинительного заключения материалы уголовного дела направлены для рассмотрения по существу в Тракторозаводский районный суд Челябинска. Об этом сообщает пресс-центр прокуратуры по Челябинской области.[4]

Основными причинами экстремизма в той или иной стране являются длительные периоды социально - экономической нестабильности, сопровождающиеся, с одной стороны, социальной дифференциацией граждан, ожесточенной борьбой за власть, растущей преступностью, а с другой - низкой эффективностью работы государственного аппарата и правоохранительных органов, отсутствием надежных механизмов правовой защиты населения. Все это ведет к нарастанию попыток разрешения возникающих противоречий и конфликтов силовым путем, причем как со стороны существующей власти, так и оппозиционно настроенных к ней элементов.

Как можно противостоять киберэкстремизму, как готовить подрастающее поколение жить в море глобальной информатизации и не утонуть в нем?

В целом в сфере образования и воспитания необходимо:

– утверждение концепции многокультурности и многоукладности российской жизни;

– проведение переподготовки школьных учителей на предмет знаний и установок в вопросах толерантности и межэтнического диалога;

– развитие воспитательной и просветительской работы с детьми и родителями о принципах поведения в вопросах веротерпимости и согласия, в том числе в отношениях с детьми и подростками;

– реагирование на случаи проявления среди детей и молодежи негативных стереотипов, межэтнической розни и личностного унижения представителей других национальностей и расового облика;

– пресечение деятельности и запрещение символики экстремистских групп и организаций в школах и вузах;

– индивидуальная работа с теми, кто вовлечен в деятельность подобных групп или разделяет подобные взгляды;

– расширение для школьников экскурсионно-туристической деятельности для углубления их знаний о стране и ее народах;

– развитие художественной самодеятельности на основе различных народных традиций и культурного наследия, а также создание современных мультимедийных продуктов о культурном многообразии России.

Кроме того, крайне важно использовать содержание обществоведческих курсов, курсов истории и права. Например, в обществознании при изучении таких тем, как «Многообразие современного мира», «Глобализация и ее последствия, «Сетевые структуры в современной мировой политике», «Целостность и противоречивость современного мира», «Общество и человек перед лицом угроз и вызовов XXI века» целесообразно использовать метод индивидуальных и групповых проектов. Метод проектов позволяет всесторонне и системно исследовать проблему; получить практические результаты; сформировать у обучающихся комплекс мыслительных способностей (понимания, рефлексии, конструирующего воображения, способности к целеполаганию и т.д.); создать образ целостного знания; повысить мотивацию обучающихся в получении дополнительных знаний; изучить важнейшие методы научного познания (выдвинуть и обосновать замысел, самостоятельно поставить цель проекта, определить круг задач, необходимых для решения проблемы, найти метод анализа ситуации); воспитать значимые общечеловеческие ценности (социальное партнерство, толерантность, диалог, чувство ответственности, самодисциплины, желания делать свою работу качественно); развивать исследовательские и творческие способности личности, способность к самоопределению и целеполаганию, умению самостоятельно конструировать свои знания, коммуникативные умения и навыки (в том

числе и участие в групповой работе), умение работать с различными информационными источниками.

Сущность и ценность образовательных проектов состоит в том, чтобы научить детей формировать свою точку зрения на решения того или иного социокультурного вопроса.

В соответствии с доминирующим методом или видом деятельности можно выделить следующие типы проектов:

1.Прикладные проекты, которые отличает четко обозначенный с самого начала результат деятельности его участников. Проекты такого вида предполагают тщательное продумывание структуры, распределение функций между участниками, оформление итогов деятельности с их последующей презентацией и внешним рецензированием.

2.Исследовательские проекты, которые подразумевают деятельность обучающихся по решению творческих задач с заранее неизвестным результатом и предполагают наличие основных этапов, характерных для любой научной работы.

3.Информационные проекты, которые направлены на изучение характеристик каких- либо процессов, явлений, объектов и предполагают их анализ и обобщение выявленных фактов (связь с исследовательской работой).

4.Ролево-игровые проекты, в которых участники исполняют определенные роли (литературных персонажей или выдуманных героев), обусловленные характером и содержанием проекта, имитирующие социальные или деловые отношения. Такая работа способствует приобретению социального опыта обучающимися.

В этой связи интересными могут быть следующие темы проектов:

- Международный терроризм как относительно новая угроза человеческому развитию.
- Эссе на тему «Терроризм - угроза XXI века».
- IT-терроризм как угроза экономической безопасности в условиях глобализации.
- Терроризм - глобальная проблема мира.
- Терроризм - угроза национальной безопасности России.
- Терроризм – глобальная проблема современности.
- Терроризм как угроза национальной безопасности.

Публикация выполнена при поддержке гранта РГНФ № 13-06-00156 «Подготовка педагогических кадров к профилактике и противодействию идеологии киберэкстремизма среди молодежи».

Библиографический **список**

1. Denning D. Cyberterrorism // Penn State Law Review. – Vol. 110(2000). – Mode of access.:http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html.

2. Gordon S. Cyberterrorism? // Symantec Security Responce. – 2010. – Mode of access.:
http://www.packetsource.com/article/laws-and-regulations/39683/cyberterrorism
3. Первый Пермский правовой портал. - URL-ссылка: http://territoriaprava.ru/topics/34572.
4. Сайт информационного агентства "Урал-пресс-информ". – URL-ссылка:http://uralpress.ru/news/2011/04/06/sud-nakazhet-16-letnego-ekstremista-v-kontakte.
5.Современный политический экстремизм: понятие, истоки, причины, идеология, организация, практика, профилактика и противодействие. Рук. авт. колл. Дибиров А.-Н.З., Сафаралиев Г.К. Махачкала. 2009г. Реферат. - URL-ссылка: http://do2.gendocs.ru/docs/index-404168.html

Карманова Е.В.
к. п. н., доц. кафедры информатики
Туркова Е.С,
студентка факультета информатики.

МЕТОДИКА ПРОВЕДЕНИЯ ВЕБ-СЕМИНАРА ПО ТЕМЕ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» ДЛЯ УЧАЩИХСЯ СТАРШИХ КЛАССОВ

ФГБОУ ВПО «Магнитогорский государственный университет», monitor81@mail.ru

Аннотация

В статье описываются основные положения методики проведения веб-семинара с использованием платформы Comdi в процессе изучения темы информационная безопасность учащимися старших классов. Рассмотрены основные этапы проведения веб-семинара, а также даны практические рекомендации по повышению эффективности работы участников в рамках веб-семинара.

Стремительное развитие информационных технологий, а также активное использование их в повседневной жизни требуют понимания молодежи в необходимости применения основных правил информационной безопасности. Вопросы информационной безопасности рассматриваются на уроках информатики и ИКТ в старших классах. Однако часто преподаватели используют традиционные формы и средства изучения данной темы (чтение и пересказ учебника), таким образом, материал становится для учащихся скучным и неинтересным, и, как следствие этого, учащиеся плохо усваивают данный материал и в дальнейшем имеют «пробелы» в области информационной безопасности.

На наш взгляд, данную тему можно преподавать, используя новую современную форму обучения – обучающий веб-семинар. Следует учитывать, что информатика и ИКТ, как школьная дисциплина, наряду с теоретической базой, имеет огромный прикладной характер, который выражается в многообразии изучаемого программного обеспечения. Необходимость уметь пользоваться, прикладными программами очевидна, как из требований к умениям подготовки учащихся, так и дальнейшей жизнедеятельности человека.

Веб-семинар (webinar) – разновидность web-конференции, онлайн-встреч или презентаций через интернет. Основным отличием веб-семинара от web-конференции является использование его для организации обучения. По своему предназначению обучающий веб-семинар чем-то напоминает установочную лекцию с элементами демонстрации практических методик.

Веб-семинары появились не так давно, но их использование настолько интенсивно, что уже сейчас накоплено огромное количество инструментов и средств, которые могут быть использованы в процессе проведения веб-семинара: аудио; видео; презентации; демонстрация документов; обмен файлами; электронная доска; демонстрация рабочего стола; чат; голосования и опросы; удаленный рабочий стол; совместное использование приложений.

Выбирать платформу для проведения вебинара следует исходя из возможностей, которыми обладают сервисы. Не существует однозначно лучшего сервиса – он может быть лучшим по каким-то критериям. Проведя анализ платформ, мы решили, что для данного веб-семинара будем использовать COMDI.com (рис. 1), так как у нее понятный русскоязычный интерфейс, она проста в использовании и учащимся не составит труда зарегистрироваться и посмотреть веб-семинар.

Цель веб-семинара: сформировать знания, умения и навыки о защите информации, изучить современные технологии борьбы с вредоносными программами.

Задачи веб-семинара:

1. Образовательные: дать представление о классических компьютерных вирусах и вредоносных программах, познакомить с классификацией вредоносных программ, выработать умение и навыки защиты информации.
2. Воспитательные: показать роль знаний в человеческом обществе, способствовать воспитанию ответственности за используемые и создаваемые программные продукты, совершенствовать навыки общения.

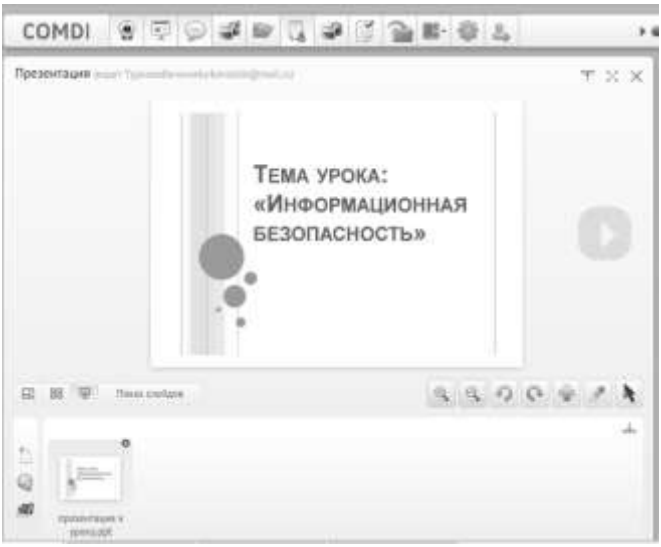


Рис. 1. Вид рабочего экрана Comdi

3. Развивающие: научить использовать телекоммуникационные средства общения в учебном процессе, сформировать опыт работы в веб-семинарах на примере платформы COMDI.

Предложенная нами методика базируется на деятельностном подходе. Выбор данного подхода обусловлен тем, что государственный стандарт по информатике предполагает приоритет данного подхода к процессу обучения, развитие у учащихся широкого комплекса общих учебных и предметных умений, овладение способами деятельности, формирующими познавательную, информационную, коммуникативную компетенции.

К специфическим принципам деятельностного подхода, подходящим именно для проведения веб-семинаров, мы отнесли:

- принцип учета ведущих видов деятельности и законов их смены предполагает применение разнообразных форм, средств и методов при организации веб-семинаров, к примеру, на наш взгляд, наиболее эффективным будет являться использование наглядных средств (презентаций), их просмотр, организация дискуссий в рамках веб-семинара, распределение индивидуальных творческих заданий.

- принцип преодоления зоны приближающегося развития и организация в ней совместной деятельности детей и взрослых. Данный принцип очень явно выражен в проведении веб-семинара, так как, проводя веб-семинары по информатике и ИКТ учащиеся и учитель очень тесно взаимодействуют между собой, задавая вопросы по теме друг другу.

В качестве основных инструментов и средств, используемых в веб-семинаре, мы предлагаем использовать презентации, опросы, голосования и чаты.

В табл. 1 представлены основные этапы проведения веб-семинара.

Таблица 1

Этапы реализации веб-семинара по теме «Информационная безопасность»

Этапы	**Ученик**	**Учитель**
Подготовительный этап	На данном этапе ученики заранее регистрируются на сайте и пробуют авторизоваться под своим логином и паролем.	1.Предварительная подготовка и проверка технического обеспечения; 2.Составление плана веб-семинара; 3.Информирование участников о правилах совместной работы (как технического, так и организационного характера); 4.Распределение ролей между участниками.
Практический этап	1.Ученики просматривают презентацию: • Слайд 1. «Термин ИБ». • Слайд 2. «Основные составляющие ИБ». • Слайд 3. «Понятия доступности, целостности и конфиденциальности». • Слайд 4 «Определения угрозы, атаки, источники угрозы». • Слайд 5. «Критерии классификации угроз». • Слайд 6. «Вредоносное программное обеспечение».	1. Распределение времени и расстановка акцентов: наиболее важным частям материала необходимо уделить больше внимания и времени; 2.Пояснение информации, данной на слайдах: 2.1.Использование курсора как указки; 2.2.Выделение во время презентации наиболее значимых слов другим цветом; 2.3.Комментирование информации, которая появляется в чате (вопросы и высказывания участников). 3.Использование жизненных примеров. 4. Объявление заранее подготовленных вопросов (как правило, в том случае, если низкая активность в чате): 4.1. Зачем нужна ИБ?

	• Слайд 7. «Какие различают впо по механизму распространения» • Слайд 8. «Что такое Антивирусная программа (антивирус)». • Слайд 9. «Недостатки антивирусных программ». 2. Слушают учителя, задают и отвечают на вопросы по данной теме в чате, который учитель заранее организует. 3. Решают практическое задание. Правильный ответ: Знания основ информационной безопасности залог будущего успеха! 4. Участвуют в голосовании.	4.2. Что такое доступность, целостность и конфиденциальность? 4.3. Какие вы знаете антивирусные программы? 4.4. Каковы мотивы и цели компьютерных преступлений? 4.5. Что такое криптографические методы? 4.6. Какие законы в области информационной безопасности существуют в нашей стране и в мире? 5. Представление практического задания: “Расшифруйте сообщение Е зашифрованное с помощью шифра Цезаря: Офжфпё хшфхи пфыхчужэпхффхр злохцжшфхшщп ожтхй зъкъалйх ъшцльж! Используйте ROT 7.” 6. Организация голосования по теме «Самая распространенная антивирусная система»: • Касперский • Dr. Web • F-Secure McAfee • Nod32 • Norton Symantec • Panda • Avast • E-Trust • другая.
Заключительный этап		На заключительном этапе учитель подводит итоги проведения веб-семинара. Определяет самых активных участников веб-семинара. Благодарит всех за участие в веб-семинаре.

Отметим, что в рамках веб-семинаров следует придерживаться следующих правил:

- Каждые 5, максимум 10 минут необходимо задавать вопросы.
- Менять пассивные-теоретические слайды как можно чаще (максимум через 3-4 минуты).
- Активно использовать интонации своего голоса.
- Применять средства рисования платформы (при условии их наличия), переходя от презентации к «белой доске».
- Пресекать все непродуктивные темы общения в чате.
- Необходимо «вытягивать» ответы из участников, заставлять их участвовать в работе.
- Не затягивать веб-семинар, придерживаться установленного плана.

Таким образом, описанная методика проведения веб-семинара по теме информационная безопасность среди учащихся старших классов позволит повысить уровень обученности учащихся по данной теме, повысить мотивы к дальнейшему изучению данной темы, а также разнообразит традиционные формы, используемые в учебном процессе, сделает процесс изучения темы интересной и познавательной.

Публикация выполнена в рамках проекта РГНФ № 11-06-01006 «Разработка и апробация модели подготовки научно-педагогических кадров к обеспечению информационной безопасности в ИКТ-насыщенной среде».

Библиографический список

1. Фролов. Ю.В. Подготовка и проведение вебинаров: учеб.-метод. пособие для преподавателей, студентов и слушателей системы повышения квалификации. – М.: МГПУ, 2011. – 30 с.
2. Шелепаева. А.Х. Поурочные разработки по информатике : учеб. – метод. пособие. – М.: ВАКО, 2006.- 272 с.
3. Чусавитина Г.Н. Применение интегративных механизмов при подготовке будущих учителей в области обеспечения информационной безопасности // Вестник компьютерных и информационных технологий, № 5, 2010. С. 49-54.

Макашова В.Н.
к. *п. н., доц. каф. информационных технологий*

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ

ФГБОУ ВПО «Магнитогорский государственный университет»,
makashova.vera@mail.ru

Наличие мощной информационно - ресурсной базы, пересечение многочисленных информационных потоков, имеющих не только

внутреннее, общероссийское, но и международное значение, обусловливает особую актуальность проблем информационной безопасности, предполагает решение комплекса проблем по созданию развитой и защищенной информационной среды, становится одним из важнейших направлений обеспечения общей безопасности образовательных учреждений.

Переход на электронную обработку информации создаёт угрозы целостности, доступности информации, а использование сети Интернет многократно повышает опасность утечки персональных данных и конфиденциальной информации, хакерских и других атак. Вместе с этим увеличивается объем жизненно важных для образовательного учреждения конфиденциальных данных об учениках, их родителях, сотрудниках, результатах деятельности, обрабатываемых в различных информационных системах и передаваемых с помощью различных каналов связи. Одним из наиболее сложных вопросов остается обеспечение защиты передаваемых персональных данных, необходимых для отправки и обработки в различные государственные структуры, а так же взаимодействие с, органами управления, партнерами. Актуальной и важной является проблема обеспечения сохранности служебных данных, таких как базы ЕГЭ, успеваемость, комплектация, передаваемых как по сети Интернет, так и на носителях.

Большие средства выделяемые для информатизации образовательных объектов привели к тому, что все образовательные учреждения г. Магнитогорска оснащены компьютерной и оргтехникой, объединенных в локальную сеть. Локальные сети образовательных учреждений построены на различной физической архитектуре, с применением проводных и беспроводных технологий, с организацией выделенных серверов, реализующих самые разные сервисы: электронная почта, хранилище данных, файрвол и т.д. Во многих образовательных учреждениях функционируют мини АТС, создаются виртуальные сети с оптоволоконной средой передачи, предоставляемой различными компаниями, например «Магинфо», «СвязьТелеКом», «ДомРу». Для решения вопросов развития, обслуживания и управления информационной инфраструктурой в образовательных учреждениях введены должности заместителя директора по информатизации, лаборанты компьютерных классов, инженеры, ответственные операторы баз ЕГЭ. В их обязанности входит:

– снабжение расходными материалами для средств оргтехники;

– выполнение работы по эксплуатации и администрированию различных баз данных образовательных учреждений;

– оказание технической поддержки пользователям сети;

– организация доступа к локальной и глобальной сетям;

– обеспечение контроля безопасности контента;

– внедрение новых АИС и сервисов в образовательное учреждение;

– составление инструкций по работе с сетевым программным обеспечением и доведение их до сведения пользователей;

– ведение контроля за использованием сетевых ресурсов и программного обеспечения;

– проведение анализа регистрационной информации, относящейся к сети в целом и к серверам в особенности;

– обеспечение защиты оборудования локальной сети, в том числе интерфейсов с другими сетями, обеспечение работоспособности баз данных;

– ведение контроля за выполнением резервного копирования отдельных данных;

– конфигурирование офисной АТС и поддержание ее в работоспособном состоянии;

– выполнение сопровождения и обновления версий программ АИС, антивирусов, и др.;

– своевременное предоставление данных учредителям и другим контролирующим органам;

– обеспечение защиты локальной сети от зловредного программного обеспечения (вирусы), обнаружение и ликвидация зловредного кода;

– ведение журнала системной информации, архивации, обновления и иной технической документации в письменном и электронном виде.

По мнению работников ОУ, обеспечивающих работоспособность ИТ-инфраструктуры, одной из приоритетных задач является обеспечение информационной безопасности и управление информационными рисками. Так как ИТ-инфраструктура образовательного учреждения расширяется, усложняется и оказывается доступной извне, повышается опасность утечки персональных данных и конфиденциальной информации, хакерских и других атак. К тому же территориальные органы Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзора), осуществляют контроль образовательных учреждении на предмет соблюдения законодательства о персональных данных. 27 июля 2006 г. был принят Федеральный закон № 152-ФЗ «О персональных данных», для обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну. Одной из причин принятия данного закона послужили многочисленные факты краж баз персональных данных в государственных и коммерческих структурах, их повсеместная продажа. 21 декабря 2010 г. был принят

федеральный закон № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию». Этот закон внёс в другие федеральные законы ряд положений, предполагающих фильтрацию интернет-сайтов по системе чёрно/белого списка и блокировку запрещённых Интернет-ресурсов. Необходимо отметить, что нарушение конфиденциальности персональных данных субъектов образовательного учреждения может повлечь административную и уголовную ответственность.

В этих условиях возникает проблема обеспечения эффективной защиты данных, для чего необходимо построение комплексной системы управления информационной безопасностью (СУИБ) и подготовка к сертификации на соответствие международным стандартам обеспечения информационной безопасности (ИБ). Однако сегодня ситуация такова, что в большинстве российских образовательных учреждения вопросам информационной безопасности не уделяют должного внимания, преобладают стихийно сложившиеся, в основном технические и физические процедуры защиты данных, отсутствуют формализованные процессы управления рисками информационной безопасности. Одной из наиболее ответственных и сложных задач, решаемых в процессе создания СУИБ, является анализ информационных рисков, который позволяет ответить на вопрос: что и от кого нужно защищать в образовательном учреждении. Результаты грамотно проведённого анализа рисков помогают оптимизировать затраты на обеспечение безопасности за счёт направления средств для устранения наиболее критичных уязвимостей и защиты значимых ресурсов и сервисов для образовательного учреждения.

По мнению экспертов, в образовательных учреждениях существует ряд сдерживающих факторов, связанных с обеспечением информационной безопасности. К ним относятся:

– финансирование мер по обеспечению ИБ по остаточному принципу из-за трудностей при обосновании необходимости вложений в средства защиты;

– незнание и несоблюдение сотрудниками (секретарь, кадровик, оператор БД, учителя) правил работы с ценной информацией и режима ИБ;

– отсутствие Политики безопасности образовательного учреждения;

– периодические сбои в работе АИС, возникающие из-за ошибок пользователей, различия в конфигурации и частых обновлений, присылаемых учредителями;

– отсутствие полной и подробной документации по работе с АИС и сервисами функционирующими в образовательном учреждении;

– отсутствие формализованной классификации информации по степени ее критичности.

За последние десятилетия создан ряд стандартов и подходов к обеспечению информационной безопасности и управлению информационными рисками. Наибольшую известность в мировой практике управления информационными рисками имеют такие международные спецификации и стандарты как ISO 17799–2002 (BS 7799), ISO/IEC 27002, GAO и FISCAM, SCIP, COBIT, NIST 800–30, SAC, COSO, SAS 55/78 и другие [1].

Самым распространенным является стандарт США NIST 800-30 подробно затрагивающий вопросы управления информационными рисками. Считается, что система управления рисками должна минимизировать возможные негативные последствия, связанные с использованием информационных технологий, и обеспечить выполнение основных процессов. Согласно стандарту NIST 800-30 управление рисками состоит из 9 стадий.

1. Описание системы. На данном шаге определяются границы системы, функции системы, критичные элементы ИС, классификация данных с позиции ИБ.
2. Идентификация угроз. Составляется перечень угроз характерных для данной ИС на основе имевших место инцидентов в области ИБ, данных по инцидентам в аналогичных системах.
3. Идентификация уязвимостей. На основе требований в области ИБ и данных по аудиту данной ИС формируется список потенциальных уязвимостей.
4. Анализ системы управления ИС. На данном шаге анализируется система управления с позиции возможного воздействия на выявленные угрозы и уязвимости.
5. Оценка параметров угроз. Определяется вероятность реализации потенциальной уязвимости, которая приведет к инциденту.
6. Анализ возможных последствий нарушения режимов ИБ. На данном шаге выбирается система критериев для оценки последствий нарушения режима ИБ и принимается интегрированная шкала для оценки тяжести последствий, в результате получается ранжированные по степени опасности последствия нарушения ИБ.
7. Определение рисков. Измеряется уровень рисков нарушения конфиденциальности, целостности и доступности информационных ресурсов. Уровень риска зависит от уровней угроз, уязвимостей и цены возможных последствий.
8. Выработка рекомендаций по управлению рисками. Рекомендации должны быть комплексными и учитывать возможные меры различных уровней, например, внесение изменений в политику ИБ,

изменения в регламентах обслуживания и должностных инструкциях, дополнительные программно-технические средства.

9. Разработка отчётных документов [2].

На сегодняшний день существует достаточно много консалтинговых компаний, которые проводят анализ рисков в рамках услуг по аудиту информационной безопасности, однако образовательным учреждениям чаще всего приходится выполнять это собственными силами.

При проведении анализа рисков важно придерживаться принципа избирательного анализа и правильной организации. Избирательный анализ предполагает включение в анализ, особенно на первом этапе, только наиболее критичных ресурсов, так как рассмотрение каждой рабочей станции потребует больших трудовых и временных затрат, рекомендуют сосредоточиться на основных процессах. Еще один момент, на который необходимо обратить внимание — организация оценки критичности, которая в большинстве случаев является самой сложной задачей при проведении анализа рисков. Здесь надо понять, кто эту критичность, и для каких ресурсов может оценить, какую методику использовать специалистам для оценки, чтобы результаты были сопоставимы и показательны.

Риски можно оценивать качественными и количественными методами. Качественная оценка предполагает присвоение риску значения в соответствии с выбранной шкалой, качественные методы просты для понимания и использования, но они не могут дать конкретную оценку, насколько выгодно применение комплекса контрмер и выгодно ли вообще. С помощью количественных методов с заданной точностью можно сказать о необходимых средствах и мерах защиты.

В настоящее время в мире существует несколько десятков автоматизированных средств, позволяющих провести анализ рисков. Наиболее известными реализациями являются Cobra, CRAMM, Risk Advisor, Risk Watch, BCM-Analyser, система управления информационной безопасностью «АванГард», Digital Security Office (ГРИФ, КОНДОР).

CRAMM — инструментальное средство, реализующее одноименную методику, которая была разработана компанией BIS Applied Systems Limited по заказу британского правительства. Метод CRAMM позволяет производить анализ рисков и решать ряд других аудиторских задач: обследование информационной системы, проведение аудита в соответствии с требованиями стандарта BS 7799, разработка политики безопасности.

Данная методика опирается на оценки качественного характера, получаемые от экспертов, но на их базе строит уже количественную оценку. Метод является универсальным и подходит и для больших, и

для малых организаций как правительственного, так и коммерческого сектора. CRAMM предполагает разделение всей процедуры на три последовательных этапа. Задачей первого этапа является определение достаточности для защиты системы применения средств базового уровня, реализующих традиционные функции безопасности, или необходимость проведения более детального анализа. На втором этапе производится идентификация рисков и оценивается их величина. На третьем этапе решается вопрос о выборе адекватных контрмер. Для каждого этапа определяются набор исходных данных, последовательность мероприятий, анкеты для проведения интервью, списки проверки и набор отчетных документов.

Достоинства метода CRAMM: хорошо структурированный и широко опробованный метод анализа рисков, может использоваться на всех стадиях проведения аудита безопасности информационных систем, объемная база знаний по контрмерам в области ИБ. Гибкость и универсальность метода позволяют его использовать для аудита информационной системы любого уровня сложности и назначения, позволяет разрабатывать план непрерывности бизнеса. К недостаткам метода CRAMM можно отнести следующие:

– для его использования требуется высококвалифицированный аудитор;

– аудит по данному методу процесс достаточно трудоемкий и может потребовать месяцы непрерывной работы;

– генерирует большое количество бумажной документации, которая не всегда оказывается полезной на практике;

– невозможно внести дополнения в базу знаний CRAMM, что вызывает определенные трудности при адаптации этого метода к потребностям конкретной организации.

Концептуальная схема проведения обследования по методу CRAMM показана на рис. 1.

Программное обеспечение RiskWatch, разрабатываемое американской компанией RiskWatch, Inc., фактически является американским стандартом в области анализа и управления рисками. Продукт предназначен для идентификации и оценки защищаемых ресурсов, угроз, уязвимостей и мер защиты в сфере компьютерной и «физической» безопасности предприятия. Аналогично методу CRAMM, RiskWatch использует в качестве критериев для оценки и управления рисками предсказания годовых потерь (Annual Loss Expectancy – ALE) и оценку возврата от инвестиций (Return on Investment – ROI). RiskWatch помогает провести анализ рисков и сделать обоснованный выбор мер и средств защиты. Используемая в программе методика включает в себя 4 фазы.

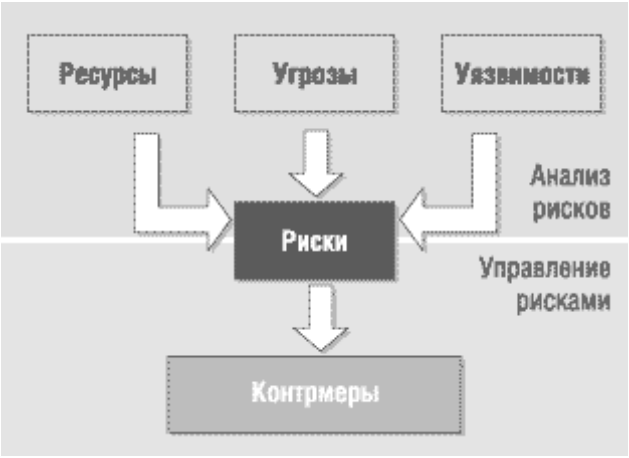


Рис. 1. Схема проведения обследования по методу CRAMM

Первая фаза — определение предмета исследования, на данном этапе описываются параметры организации (тип организации, состав исследуемой системы, базовые требования в области безопасности). Вторая фаза — ввод данных, описывающих конкретные характеристики системы (ресурсы, потери и классы инцидентов, частота возникновения каждой из выделенных угроз, степень уязвимости и ценность ресурсов). Третья фаза — оценка рисков на основе связи между ресурсами, потерями, угрозами и уязвимостями, выделенными на предыдущих этапах. Дополнительно рассматриваются сценарии «что если...», которые позволяют описать аналогичные ситуации при условии внедрения средств защиты. Четвертая фаза — генерация отчетов (отчет о стоимости защищаемых ресурсов, отчет об угрозах и мерах противодействия т.д). Для отечественных пользователей проблема заключается в том, что получить используемые в RiskWatch оценки (такие как LAFE и SAFE) для наших условий достаточно проблематично. Хотя сама методология может с успехом применяться и у нас.

COBRA - Consultative Objective and Bi-Functional Risk Analysis является средством анализа рисков и оценки соответствия стандарту BS7799, реализующим методы количественной оценки рисков, а также инструменты для консалтинга и проведения обзоров безопасности. При разработке инструментария COBRA были использованы принципы построения экспертных систем, обширная база знаний по угрозам и уязвимостям и большое количество вопросников. В семейство программных продуктов COBRA входят также COBRA ISO17799 Security Consultant, COBRA Policy Compliance Analyst и COBRA Data Protection Consultant. Анализ рисков, выполняемый данным методом, соответст-

вует базовому уровню безопасности, т.е. уровни рисков не определяются. Достоинством методики является простота. Необходимо ответить на несколько десятков вопросов, затем автоматически формируется отчет.

Risk Advisor позиционируется как инструментарий аналитика или менеджера в области информационной безопасности. В нём реализована методика, позволяющая задать модель информационной системы с позиции информационной безопасности, идентифицировать риски, угрозы, потери в результате инцидентов. Есть возможность получать информацию о новых и актуальных угрозах с миллионов точек сбора информации. Данный инструмент позволяет документировать всевозможные аспекты, связанные с управлением риском на верхних уровнях — административном и организационном. Программно-технические аспекты описывать в данной модели не очень удобно. Оценки даются в качественных шкалах, подробного анализа факторов рисков не предусмотрено. Сильной стороной данного метода является возможность описания разноплановых взаимосвязей, адекватного учета многих факторов риска.

Комплексная экспертная система управления информационной безопасностью «Авангард», разработанная институтом системного анализа РАН, является программным продуктом, предназначенным для решения задач управления безопасностью в больших территориально-распределенных автоматизированных информационных системах, и призвана облегчать задачи контроля за центральными структурами уровня обеспечения информационной безопасности на местах. Данный комплекс является одним из самых мощных инструментов анализа и контроля рисков отечественного производства. Основные возможности комплекса: гибкая система ввода и редактирования модели предприятия, возможность построения модели рисков, система оценки и сравнения рисков, оценка мер противодействия, построение вариантов комплексов мер защиты и оценка остаточного риска. Программный комплекс «Авангард» призван играть вспомогательную роль в решении задач управления информационной безопасности, а именно обеспечивать полноценный всесторонний анализ, позволяющий сформулировать обоснованный набор целей безопасности, обосновать политику безопасности, гарантировать полноту требований безопасности, контроль выполнения которых нужно осуществлять.

Digital Security Office - система управления информационными рисками и оценки соответствия системы управления ИБ международным, национальным и корпоративным стандартам в области информационной безопасности. Продукт состоит из системы анализа рисков ГРИФ и системы для оценки соответствия системы управления ИБ требованиям стандартов КОНДОР. Система ГРИФ позволяет постро-

ить приближенную модель информационной системы, содержащую наиболее критичные ресурсы и основные угрозы и уязвимости, с учетом вероятности их реализации. Полученная модель показывает наиболее уязвимые места ИС, уровень ущерба, к которому может привести каждая уязвимость, а также позволяет принять решение о том, какие контрмеры будут наиболее эффективны. В нем разработано гибкое и, несмотря на скрытый от пользователя сложнейший алгоритм, учитывающий более 100 параметров, максимально простое в использовании программное решение, основная задача которого дать возможность ИТ-менеджеру самостоятельно (без привлечения сторонних экспертов) оценить уровень рисков в информационной системе и эффективность существующей практики по обеспечению безопасности компании. Данный комплекс делает оценку рисков по различным информационным ресурсам, подсчитывает суммарный риск по ресурсам компании, а также ведет подсчет соотношения ущерба и риска и выдает недостатки существующей политики безопасности. В системе есть модуль управления рисками, который позволяет проанализировать все причины того значения риска, который получается после обработки алгоритмом занесенных данных. Здесь можно задать контрмеры, их стоимость и влияние на уровень риска.

Система КОНДОР включает в себя базы стандартов управления информационной безопасностью (ISO 17799:2000, ISO 17799:2005, ISO 27001, СТО БР ИББС-1.0-2006), представленных в виде перечня требований. Анализируя выполнение каждого требования, система, формируя отчёт, позволяет получить полную картину - какие положения стандартов выполняются, а какие нет. Также в системе предусмотрена возможность создавать свои базы требований, чтобы провести оценку соответствия, например, корпоративному стандарту безопасности. В отчете отражаются все положения политики безопасности, которые соответствуют и не соответствуют стандарту, а также существующий уровень риска невыполнения требований политики безопасности в соответствии со стандартом. Элементам, которые не выполняются, даются комментарии и рекомендации экспертов. По желанию специалиста, работающего с программой, могут быть выбраны генерация отчета, например, по какому-то одному или нескольким разделам стандарта ISO 17799, общий подробный отчет с комментариями, общий отчет о состоянии политики безопасности без комментариев для представления руководству. Все варианты отчетов для большей наглядности сопровождаются диаграммами. КОНДОР дает возможность специалисту отслеживать вносимые на основе выданных рекомендаций изменения в политику безопасности, постепенно приводя ее в полное соответствие с требованиями стандарта. Существует возможность сравнения отчетов на разных этапах внедрения комплекса мер по

обеспечению защищенности. Данная система реализует метод качественной оценки рисков по уровневой шкале рисков: высокий, средний, низкий.

Качественное проведение анализа рисков информационной безопасности поможет определить цели управления информационной безопасностью, оценить основные критичные факторы, негативно влияющие на ключевые процессы образовательного учреждения, и выработать осознанные, эффективные и обоснованные решения для их контроля или минимизации.

Следующим этапом процесса управления информационными рисками является обработка выявленных рисков. Обработка информационных рисков – это этап, в процессе которого определяется, какие действия по отношению к рискам требуется выполнить. Основными способами обработки рисков являются: принятие рисков, уклонение от рисков, передача рисков, снижение рисков. Принятие рисков осуществляется в том случае, если уровень рисков признается приемлемым. Т.е. образовательное учреждение не считает целесообразным применять какие-либо меры по отношению к этим рискам и готово понести ущерб. Уклонение от рисков – это полное устранение источника риска. Передача рисков – перенесение ответственности за риск на третьи лица (например, поставщику оборудования или страховой компании) без устранения источника риска. Снижение рисков – это выбор и внедрение мер по снижению вероятности нанесения ущерба.

В процессе обработки рисков сначала требуется определить, какие риски требуют дальнейшей обработки, а какие можно принять. Необходимо свести выявленные риски в реестр, например, в таблицу (табл.1), проранжировав их по уровню, учитывая значения рисков, реализации угроз через уязвимости, необходимо указать возможные контрмеры. Контрмеры могут снизить уровни рисков различными способами:

– уменьшая вероятность осуществления угроз безопасности;

– ликвидируя уязвимости или понижая их величину;

– уменьшая величину возможного ущерба;

– способствуя восстановлению ресурсов АС, которым был нанесен ущерб;

– выявляя атаки и другие нарушения безопасности [2].

Таблица 1.

Пример таблицы описания рисков и контрмер для снижения рисков

Уязвимость	Рисковое событие, угроза	Уровень риска	Последствия наступления рискового события	Контрмеры

Программное обеспечение	Вирус	Высокий	Сбой ПО, нарушение работы образовательного учреждения	Установка антивирусного ПО, своевременные обновления
Базы данных	Хакерская атака	Высокий	Утечка конфиденциальной информации	Установка файрвола, своевременное обновление системного ПО
…				

С точки зрения нормативной документации политики информационной безопасности, на уровне образовательного учреждения должна быть разработана концепция информационной безопасности, которая представляет собой перечень общих принципов и задач по защите основных процессов. Стандарт ISO 17799:2005 (раздел 5.1.1) описывает примерную структуру этого документа и рекомендует отражать следующую информацию:

– общая характеристика объекта защиты (описание критичных ресурсов, сервисов и бизнес-процессов);

– цели и задачи создания системы защиты информации, пути их достижения;

– перечень сведений, подлежащих защите;

– основные виды угроз информационной безопасности;

– описание контрольных механизмов, оценка и управление рисками;

– основные методы защиты информационных систем;

– распределение зон ответственности за обеспечение ИБ;

– способы реагирования на форс-мажорные ситуации.

На основе общей концепции разрабатываются политики информационной безопасности – более узкоспециализированные документы. Каждый такой нормативный документ относится к какой-либо области обеспечения ИБ (политика управления паролями, политика управления доступом к ресурсам) и определяет ответственных лиц за безопасность функционирования образовательного учреждения, порядок действий, систему мер, полномочия и ответственность лиц и структур в отношении безопасности, использование программно-технических средств защиты, порядок контроля выполнения требований и др. Учитывая особенности информационной системы, бизнес-процессов образовательного учреждения, можно предложить примерный пере-

чень политик по отдельным направлениям информационной безопасности:

– комплексный план защиты информационных ресурсов образовательного учреждения от несанкционированного доступа;

– политика обеспечения безопасности удаленного доступа к ресурсам образовательного учреждения (чаще всего через web-интерфейс).

– план обеспечения непрерывности образовательного процесса;

– политика обеспечения безопасности при взаимодействии с сетью Интернет (особое внимание уделяется фильтрации контента);

– политика и регламент резервного копирования и восстановления данных;

– антивирусная политика;

– политика установки обновлений программного обеспечения;

– процедура планирования и реализации превентивных и корректирующих мер по обеспечению ИБ;

– политика инвентаризации и реестр информационных активов.

Для того чтобы написать данные документы необходимо произвести распределение ролей на конкретные технологии и процессы.

Инструкции и регламенты являются наиболее детализированными нормативными документами, стандартизующими вопросы информационной безопасности в образовательном учреждении. В общем виде они представляют собой свод правил, определяющих порядок работы в области защиты информации. В инструкциях прописаны полномочия и обязанности определенных подразделений и ролей, схема их взаимодействия с другими подразделениями и ролями в рамках общей концепции ИБ.

В итоге должен быть сформирован комплект документов, адекватный текущему положению дел, культуре и внутренним и внешним потребностям образовательного учреждения.

Очень важно повышать осведомленность учеников и родителей в области ИБ. Это можно делать с помощью тренингов, курсов, новостных рассылок, обучающих роликов, постеров и т.д. Можно использовать готовые комплексы и учебные материалы, например компания «1С» уделяет большое внимание вопросам информационной безопасности и выпустила следующие продукты:

– методическое пособие «Обеспечение защиты персональных данных»;

– программный продукт KinderGate - родительский контроль, позволяющий контролировать использование сети Интернет несовершеннолетними детьми;

– для поддержки процесса внедрения системы контентной фильтрации создан специализированный Интернет-сервер http://skf.edu.ru.

Такую форму как тренинги и семинары можно использовать для осведомленности родителей.

Тренинги и семинары в образовательных учреждения города Магнитогорска обычно проводят учителя информатики и заместители директоров по информатизации, которые в большинстве случаев являются выпускниками факультета информатики ФГБОУ ВПО МаГУ по специальности 050202.65 «Информатика», где реализуется специализация информационная безопасность. В учебный план этой специальности входят следующие дисциплины: «Правовое обеспечение информационной безопасности», «Администрирование и безопасность компьютерных систем», «Криптографические методы защиты информации», «Организационное обеспечение информационной безопасности», «Программно-аппаратные средства обеспечения информационной безопасности», «Теория информационной безопасности и методологии защиты информации», в рамках педагогической практики студенты проводят внеклассные мероприятия, направленные на повышение компетенций в области информационной безопасности учеников, преподавателей, родителей с применением метода проектов (http://wiki.iteach.ru/). Приведем темы некоторых проектов: интернет-зависимость в современном обществе; киберпреступность пришла, чтобы оставить след; сетикет, борьба с троллингом; политический инжиниринг, как вид манипуляции людьми; свобода слова; влияние интернета на молодежь; и др.

В городе имеется опыт проведения родительских собраний и педагогических советов по вопросам информационной безопасности, где выступают приглашенные специалисты вуза, консалтинговых компаний предоставляющих услуги аудита ИБ и др. компетентных лиц.

При этом надо учитывать, что обучение сотрудников основам информационной безопасности значительно отличается от обучения любым другим знаниям в первую очередь по следующим причинам:

– сотрудники не заинтересованы в обучении, т.к. это не повышает значимости и стоимость их как специалистов на рынке труда;

– правила в области информационной безопасности в основном носят ограничительный или запретительный характер и мешают пользователям в работе с популярными сервисами;

– необходимость выполнения правил не всегда очевидна, т.к. сотрудники не думают о возможных результатах, а иногда и просто о них не знают.

Обучение учащихся безопасной работе в Интернет так же является очень важной задачей. Учащиеся создают имена пользователей и

пароли для доступа на сайт школы, игровые сайты, в социальные сети, для публикации фотографий, совершения покупок в Интернете и других операций. Учащиеся должны понимать, что многие из этих сайтов социальных сетей могут просматриваться всеми, кто имеет доступ в Интернет. В результате публикации ими некоторой информации могут стать уязвимыми как данные самих учащихся, так и данные с ресурсов образовательного учреждения, т.к. зачастую пароли совпадают. Отдельно надо отметить роль социальных сетей в процессе обеспечения информационной безопасности. Социальные сети сейчас обошли по популярности блоги среди большинства подростков, однако многие дети по-прежнему ведут свой блог на своем сайте социальной сети. Недавние исследования показали, что на сегодняшний день примерно половину всех блогов пишут подростки, при этом каждые двое из троих указывают свой возраст, каждые трое из пяти сообщают о месте своего проживания и дают контактную информацию, а каждый пятый указывает свое полное имя. Разглашение подробной личной информации сопряжено с риском. Особое внимание учащихся необходимо уделять правам интеллектуальной собственности в сети Интернет.

Реализация информационных угроз может привести к подрыву авторитета образовательного учреждения, созданию в коллективе атмосферы напряженности и нестабильности, снижению уровня образовательной деятельности и темпов научно-технических исследований, утечке информации, составляющей интеллектуальную собственность, ограниченного доступа, подлежащей защите в рамках требований Конституции и российских законов. Нельзя сказать, что в образовательных учреждениях не решаются вопросы, связанные с информационной безопасностью, наоборот каждым отдельным аспектом уделяют много внимания, но на наш взгляд вопросам комплексного использования средств обеспечения информационной безопасности, внимания уделяется недостаточно. Особенно это актуально для государственных образовательных учреждений, которые в силу различных причин, в большинстве случаев, не могут позволить себе содержать высококвалифицированного специалиста в области информационной безопасности и поэтому нуждаются в постоянной методической поддержке процесса обеспечения и обучения персонала широкому комплексу вопросов в области информационной безопасности.

Публикация выполнена в рамках проекта РГНФ № 11-06-01006 «Разработка и апробация модели подготовки научно-педагогических кадров к обеспечению информационной безопасности в ИКТ-насыщенной среде».

Библиографический список

1. Биячуев. Т.А. Безопасность корпоративных сетей. / под ред. Л.Г. Осовецкого. – СПб; СПбГУ ИТМО, 2004.- 161 с.

2. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность / Петренко С.А., Симонов С.В. - М.: Компания АйТи; ДМК Пресс, 2004. - 384 с.: ил. - (Информационные технологии для инженеров).

3. Разработка нормативно-технической документации в сфере ИБ − Режим доступа: http://www.vp.verysell.ru/services/services_06/services_01_05/

4. Конеев И. Политики информационной безопасности − Режим доступа: http://www.osp.ru/cio/2007/11/4569379/

5. Чусавитин М.О. Управление рисками безопасности образовательно-информационной среды с использованием Digital Security Office // Материалы XIX Международной конференции «Применение новых технологий в образовании». Троицк, 2009. – С. 518 – 521.

6. Чусавитина Г.Н. Применение интегративных механизмов при подготовке будущих учителей в области обеспечения информационной безопасности // Вестник компьютерных и информационных технологий, № 5, 2010. - С. 49-54.

7. Чусавитина Г.Н. Информационная безопасность в открытом образовании// Информационная безопасность в открытом образовании. Магнитогорск, 2011. – С. 5 – 10.

8. Чусавитина Г.Н. Автоматизация оценки уровня защищенности информационных ресурсов образовательного учреждения с учетом стандартов ISO 17799:2005 и ISO 27001// Информационная безопасность региона: гуманитарные и технические аспекты: сб. материалов Второй всерос. науч. практ. конф. Екатеренбург, 2009. – С. 249 – 252.

Махмутов Г. Р.
магистрант

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНТЕГРАЦИИ БИЗНЕС-ПРОЦЕССОВ КОМПАНИИ В СРЕДУ ЭЛЕКТРОННОГО БИЗНЕСА

ФГБОУ ВПО «Магнитогорский государственный университет»,
glmak@gmail.ru

Аннотация

В статье определены понятия электронный бизнес, архитектура электронного бизнеса, рассмотрены вопросы интеграции бизнес-процессов компании в среду электронного бизнеса на сегодняшний день и на перспективу, представлены технологии обеспечения информационной безопасности в процессе интеграции: криптография и ее методы, а именно, шифрование, цифровая подпись, сертификат; протокол SSL и стандарт SET.

В настоящее время, когда Интернет стал неотъемлемой частью бизнеса, общения, отдыха людей и местом работы с большим количеством разнообразной информации, компании создают свои Интернет-сайты магазины и другие системы в Интернете, для того чтобы пользователи могли узнать о компании, познакомиться с ее основными целями, задачами, перечнем предоставляемых услуг.

Формируется новое экономическое пространство – новый рынок, или Интернет-рынок, как система новых экономических отношений. Как и на любом рынке, на Интернет-рынке невозможно обойтись без рекламы, без этого компания просто не выдержит возрастающей с каждым днем конкуренции. Все больше пользователей ежедневно подключается к «Всемирной паутине», в связи с этим растет как число покупателей, так и число «продавцов». В связи с возрастающей компьютеризацией и «интернетизацией» российского общества, стало актуальным использование web-сайтов для компаний, которые с помощью Интернет предоставляли бы интересующую пользователя информацию и позволяли бы решать интересующие его проблемы. Количество компаний, предлагающих услуги через Интернет увеличивается с геометрической прогрессией, что создает высокую конкуренцию в данной сфере бизнеса. В этих условиях контентная оптимизация web-сайтов становится наиболее актуальной проблемой, чем быстрее пользователь найдет web-сайт отвечающий запросам пользователя, тем больше вероятность того, что он приобретет продукцию.

Реклама в Интернет стала одной из составляющих системы повышения эффективности работы предприятия. Актуальность проведения рекламных компаний в Интернет с каждым днем становится все более очевидной. Результаты последних исследований Института рекламы показали, что использование Internet-технологий может принести реальную экономию и прибыль, поскольку реклама в Интернет, что подтверждает исследование, превосходит по действенности радио- и телевизионную рекламу. Наличие корпоративного сайта для компании, предлагающей свои услуги не только на местном уровне, но и на региональном и общероссийском выглядит не просто интересным бонусом, а просто необходимостью. Это возможность рассказать о себе, продемонстрировать свои услуги и предложения, не делая при этом, практически, каких-либо особенных усилий. Количество заинтересовавшихся клиентов будет возрастать, а для постоянных клиентов, сайт – это оптимальный способ отслеживания новостей компании, появления новых услуг и коммерческих предложений. Корпоративный сайт – необходимый инструмент успешного бизнеса любой компании. При этом электронный бизнес позволяет качественно преобразовать все бизнес-процессы, а именно:

- повысить эффективность продвижения товара/услуг на рынок

(доведение информации до потенциальных клиентов, привлечение внимания к предлагаемым товарам и к самой компании, позволяет легко и быстро информировать партнеров и клиентов о продуктах и услугах);

- повысить оперативность информационного обслуживания пользователей (непрерывное, круглосуточное информационное обслуживание, оперативность получения информации, особенно при международных операциях);
- снизить цены (избавиться от излишков и сократить накладные расходы связанные с обменом информацией за счет использования более дешевых средств коммуникаций);
- расширить географическую сферу информационного обслуживания;
- создавать альтернативные каналы продаж, например, через электронный магазин на корпоративном сайте;
- получить представительство на глобальном рынке.

Каждое предприятие стремиться к продвижению своей продукции, расширению рынка своих услуг, привлечению новых клиентов и удержанию постоянных с использованием возможностей сети интернет. Все очевиднее становится существенная роль интернет-технологий в бизнес-процессах не только крупных корпораций, возможности электронной среды открыты для всех компаний, вне зависимости от размеров. Следовательно, можно констатировать, что электронный бизнес не менее важен для малых и средних компаний.

Компания будет эффективно развиваться, если ее внутренняя организация прозрачна и позволяет на всех уровнях управления – стратегическом, тактическом и оперативном - видеть развитие и взаимодействие всех бизнес-процессов. Компании имеют гигантское преимущество, если выстраивают организационную структуру виртуально, а потом заполняют ее реальными ресурсами, если все процессы автоматизированы и их выполнение не зависит от конкретного сотрудника, т.е. исключено влияние «человек-проект», если эффективно организована оперативная работа и не приветствуются авральные ситуации.

Таким образом, среда электронного бизнеса является не только внешней оболочкой для процессов продажи, покупки, маркетинга, но и одной из важнейших составляющих, которая связывает отношения в рамках деловых процессов внутри компании, и отношения с внешней средой. Реализация этих процессов с технологической точки зрения с использованием среды интернет возможна и относительно не сложна.

Рассмотрим модели бизнеса, которые основаны на использовании среды интернет, или бизнес-процессы, которые могут быть интегрированы в электронную среду. Это те деловые процессы, которые

дают возможность компании выйти на непосредственный контакт с клиентом, позволив ему иметь определенную роль в компании, т.е. это новый уровень общения с клиентом. Интернет - это "везде и всегда", мы выкладываем какое-либо сообщение и оно появляется практически везде. Объявление на Web-сайте могут увидеть все, в любое время года, 24 часа в сутки и, практически, по всему миру.

Это значит, что для небольшой компании возникают четыре новых направления развития:

1.Отношения с клиентом - Customer Relations Management. В Интернет гигантское количество пользователей - потенциальных клиентов, но они могут мгновенно исчезнуть в тот момент, когда их ожидания не оправдаются теми, кто работает с ними, будь то магазин или продавец определенных услуг.

2.Необходима адаптация бизнес-стратегии к возможностям Интернета.

3.Knowledge Management (управление знаниями). Что делать и как использовать те знания, которые накапливаются в компании? Можно быть специалистом по каким-то вопросам, но если эти знания не применены, то они бесполезны.

4.Supply Chain Integration - вся сеть отношений поставщиков и потребителя должна быть интегрирована. Интернет дает владельцам Web-сайтов потрясающую возможность интегрировать деловые процессы.

Кроме того, Интернет является универсальной коммуникационной платформой, на базе которой происходит слияние многих средств передачи информации: телефония, мультимедиа-приложения и др.. [2]

Электронный бизнес подразумевает не только электронную торговлю, но и бизнес вообще, деловые процессы, внутреннюю организацию компании. Одним из важнейших факторов внедрения систем электронного ведения бизнеса является возможность скоординировать все деловые процессы, в том числе: подготовку данных; консультации и поддержку; настройку на потребителя; продажи; оплату; сервис. Причем эта интеграция происходит на единой аппаратно-программной платформе.

Задачи, стоящие перед электронным бизнесом, отражаются в его архитектуре, представленной несколькими слоями.

1. Транспортный (самый нижний слой) - доставка необходимой информации (это телекоммуникационные сети Web-hosting, Интернет-Сервис-Провайдинг).

2. Электронные инструменты, которые позволяют производить различные операции:

- построение интранет, т.е. сети внутри предприятия, для того, чтобы предприятие имело эффективную организацию, понятную

структуру и легко контролировалось;

- построение экстранет сети - это предоставление возможности для потенциального клиента "зайти" в компанию и посмотреть, чем она занимается: какие существуют деловые процессы, продукты, какие у компании планы и стратегические возможности развития, как она обходится с клиентом, сколько времени по статистике занимает обработка одного запроса и т.д. Предоставляется доступ к определенным позициям важным для клиента.

3. "Деловые процессы", которые регулируют всю жизнь компании: от заказов, закупки косвенных товаров, до маркетинга, всего спектра отношений с клиентами (удержание клиентов, их обслуживание), поддержки взаимодействия между различными подразделениями компании [2].

В целом, электронный бизнес можно определить как комплекс бизнес-отношений. И, естественно, для работы нужна определенная база информационных технологий.

Одним из важнейших условий широкого применения возможностей среды интернет было и остается обеспечение определенного уровня безопасности всех совершаемых транзакций. Это касается информации, передаваемой между пользователями, информации сохраняемой в базах данных систем, информации, сопровождающей финансовые операции.

Понятие информационной безопасности можно определить как состояние устойчивости информации к случайным или преднамеренным воздействиям, исключающее недопустимые риски ее уничтожения, искажения и раскрытия, которые приводят к материальному ущербу владельца или пользователя информации. Поскольку электронная среда полностью открыта для внешнего доступа, то значимость обеспечения информационной безопасности очень велика. Важность фактора безопасности доказывают и многочисленные исследования, проводимыми в Интернете.

Существуют различные технологии обеспечения информационной безопасности. Криптография - наука об обеспечении безопасности данных, и построенные на ее основе системы призваны решать следующие задачи:

1. Конфиденциальность. Информация должна быть защищена от несанкционированного доступа, как при хранении, так и при передаче. Доступ к информации может получить только тот, для кого она предназначена. Обеспечивается шифрованием.

2. Аутентификация. Необходимо однозначно идентифицировать отправителя, при однозначной идентификации отправитель не может отказаться от послания. Обеспечивается электронной цифровой подписью и сертификатом.

3. Целостность. Информация должна быть защищена от несанкционированного изменения, как при хранении, так и при передаче. Обеспечивается электронной цифровой подписью.

В соответствии с рассматриваемыми задачами основными методами обеспечения безопасности выступают шифрование, цифровая подпись и сертификаты.

Шифрование. Осуществляя какие- либо сделки в среде Интернет, в первую очередь, необходимо убедиться, что важная информация надежно скрыта от посторонних лиц. Этому служат технологии шифрования, преобразующие простой текст в форму, которую невозможно прочитать, не обладая специальным шифровальным ключом. Благодаря данным технологиям можно организовать безопасную связь по общедоступным незащищенным каналам Интернета [1].

Любая система шифрования работает по определенной методологии, включая в себя один или более алгоритмов шифрования (математических формул), ключи, используемые этими алгоритмами, а также систему управления ключами.

Некоторые из алгоритмов симметричных систем шифрования: ГОСТ №28147-89, DES (Data Encryption Standard), тройной алгоритм DES, Международный алгоритм шифрования IDEA, RC2, RC3, RC5, CAST.

Алгоритмы шифрования с открытым ключом получили широкое распространение в современных информационных системах. Известно несколько криптосистем с открытым ключом. Наиболее разработана на сегодня система RSA, предложенная еще в 1978 г. Алгоритм RSA назван по первым буквам фамилий его авторов: Р. Л. Райвеста (R. L. Rivest), А. Шамира (A. Shamir) и Л.Адлемана (L. Adieman). Этот алгоритм стал мировым фактически признанным стандартом для открытых систем и рекомендован МККТТ (Международный Консультативный Комитет по телефонии и телеграфии). Также используются алгоритмы: ECC (криптосистема на основе эллиптических кривых) [1].

Цифровая подпись. Шифрование передаваемых через Интернет данных позволяет защитить их от посторонних лиц. Однако для полной безопасности должна быть уверенность в том, что второй участник транзакции является тем лицом, за которое он себя выдает. В бизнесе наиболее важным идентификатором личности заказчика является его подпись. В электронной среде применяется электронный эквивалент традиционной подписи - цифровая подпись. С ее помощью можно доказать не только то, что транзакция была инициирована определенным источником, но и то, что информация не была испорчена во время передачи.

Как и в шифровании, технология электронной подписи использует либо секретный ключ (в этом случае оба участника сделки приме-

няют один и тот же ключ), либо открытый ключ (при этом требуется пара ключей - открытый и личный). И в данном случае более просты в использовании и более популярны методы с открытым ключом (такие, как RSA).

При аутентификации личности отправителя открытый и личный ключи играют роли, противоположные тем, что они выполняли при шифровании. Так, в технологии шифрования открытый ключ используется для зашифровки, а личный - для расшифровки. При аутентификации с помощью подписи все наоборот. Кроме того, подпись гарантирует только целостность и подлинность сообщения, но не его защиту от посторонних глаз. Для этого предназначены алгоритмы шифрования. Например, стандартная технология проверки подлинности электронных документов DSS (Digital Signature Standard) применяется в США компаниями, работающими с государственными учреждениями. Однако у технологии RSA более широкие возможности в силу того, что она служит как для генерации подписи, так и для шифрования самого сообщения. Цифровая подпись позволяет проверить подлинность личности отправителя: она основана на использовании личного ключа автора сообщения и обеспечивает самый высокий уровень сохранности информации [1].

Сертификаты. Как было сказано выше, основной проблемой криптографических систем является распространение ключей. В случае симметричных методов шифрования эта проблема стоит наиболее остро, поэтому при шифровании данных для передачи ключей через Интернет чаще всего используются асимметричные методы шифрования.

Асимметричные методы более приспособлены для открытой архитектуры Интернета, однако и здесь использование открытых ключей требует их дополнительной защиты и идентификации для определения связи с секретным ключом. Без такой дополнительной защиты злоумышленник может выдать себя за отправителя подписанных данных или за получателя зашифрованных данных, заменив значение открытого ключа или нарушив его идентификацию. В этом случае каждый может выдать себя за другое лицо. Все это приводит к необходимости верификации открытого ключа. Для этих целей используются электронные сертификаты.

Электронный сертификат представляет собой цифровой документ, который связывает открытый ключ с определенным пользователем или приложением. Для заверения электронного сертификата используется электронная цифровая подпись доверенного центра - ЦС (Центра Сертификации). Исходя из функций, которые выполняет ЦС, он является основным компонентом всей инфраструктуры открытых ключей (ИОК или PKI — Public Key Infrastructure). Используя откры-

тый ключ ЦС, каждый пользователь может проверить достоверность электронного сертификата, выпущенного ЦС, и воспользоваться его содержимым.

Для того чтобы сертификатам можно было доверять, независимая организация, выполняющая функции ЦС и являющаяся их источником, должна быть достаточно авторитетной. В настоящее время наиболее известным источником сертификатов являются компании Thawte (www.thawte.com) и VeriSign (www.verisign.com), однако существуют и другие системы, такие как World Registry (IBM), Cyber Trust (GTE) и Entrust (Nortel). В России дистрибьютором сертификатов SSL компании Thawte сегодня является «РосБизнесКонсалтинг» (www.rbc.ru) [1].

Технология цифровых сертификатов работает следующим образом. Чтобы воспользоваться сертификатом, потенциальный покупатель должен, прежде всего, получить его в надежном источнике. Для этого ему необходимо каким-то образом доказать подлинность своей личности, возможно, явившись в эту организацию и предъявив соответствующий документ, а также передать источнику сертификатов копию своего открытого ключа. После этого при желании купить что-либо через Интернет, ему будет достаточно добавить к заказу свою электронную подпись и копию сертификата. Отдел обслуживания покупателей фирмы, в которой он совершил покупку, проверяет сертификат, чтобы убедиться, что к заказу приложен подлинный открытый ключ, а также выясняет, не аннулирован ли сертификат.

Следует отметить, что технология цифровых сертификатов является двунаправленной. Это значит, что не только фирма может проверить подлинность заказа покупателя, но и сам покупатель имеет возможность убедиться, что он имеет дело именно с той фирмой, за которую она себя выдает. Осуществив взаимную проверку, обе стороны спокойно заключают сделку, так как обладают подлинными открытыми ключами друг друга и, соответственно, могут шифровать передаваемые данные и снабжать их цифровой подписью. Такой механизм обеспечивает надежность сделки, ибо в этом случае ни одна из сторон не сможет отказаться от своих обязательств.

*Протоколы и стандарты безопасности***.** Описанные выше методы обеспечения информационной безопасности являются основой построения большинства систем в электронной среде. Это могут быть системы электронного бизнеса, обмена информацией или платежные системы. Важность вопросов безопасности для их организации очень велика. Так, согласно проводимым исследованиям, одной из основных причин медленного роста электронного бизнеса сегодня остается озабоченность покупателей надежностью средств, применяемых при расчетах в Интернете. Основные причины обеспокоенности связаны со

следующими факторами: отсутствие гарантии конфиденциальности; недостаточный уровень проверки (аутентификации) участников операции; нет гарантии целостности данных [1].

Наиболее распространенными механизмами, призванными устранить указанные факторы и обеспечить безопасность проведения электронных платежей через Интернет сегодня являются:

- протокол SSL (Secure Socket Layer), обеспечивающий шифрование передаваемых через Интернет данных;
- стандарт SET (Secure Electronic Transactions), разработанный компаниями Visa и MasterCard и обеспечивающий безопасность и конфиденциальность совершения сделок при помощи пластиковых карт.

Протокол SSL и стандарт SET. Протокол SSL - один из существующих протоколов обмена данными, обеспечивающий шифрование передаваемой информации. В настоящее время это наиболее распространенный метод защиты электронных транзакций в Интернете.

Протокол SSL является стандартом, основанным на криптографии с открытыми ключами. Протокол обеспечивает защиту данных, передаваемых в сетях TCP/IP по протоколам приложений за счет шифрования и аутентификации серверов и клиентов. Это означает, что шифруется вся информация, передаваемая и получаемая web-браузером, включая URL-адреса, все отправляемые сведения (такие, как номера кредитных карт), данные для доступа к закрытым web-сайтам (имя пользователя и пароль), а также все сведения, поступающие с web-серверов.

Протокол SSL позволяет решить часть названных проблем безопасности, однако его роль в основном ограничивается обеспечением шифрования передаваемых данных. Поэтому для комплексного решения перечисленных выше проблем была разработана спецификация и создан набор протоколов, известные как стандарт SET (Secure Electronic Transaction) — безопасные электронные транзакции [1].

Благодаря использованию цифровых сертификатов и технологий шифрования, SET позволяет как продавцам, так и покупателям производить аутентификацию всех участников сделки. Кроме того, SET обеспечивает надежную защиту номеров кредитных карт и другой конфиденциальной информации, пересылаемой через Интернет, а открытость стандарта позволяет разработчикам создавать решения, которые могут взаимодействовать между собой. Также важным фактором, обеспечивающим продвижение SET, является его опора на существующие карточные системы, ставшие привычным финансовым инструментом с отлаженной технологией и правовым механизмом.

В основе системы безопасности, используемой SET, лежат стандартные криптографические алгоритмы DES и RSA. Инфраструктура

SET построена в соответствии с инфраструктурой открытого ключа (Public Key Infrastructure, PKI) на базе сертификатов, соответствующих стандарту X.509, утвержденному организацией по стандартизации (ISO) [1].

Главная особенность SET - регламентация использования системы безопасности, которая устанавливается международными платежными системами. Требования Visa и Europay к центру обработки на основе SET включают, во-первых, традиционные требования к обработке пластиковых карт (защита помещений, контроль над доступом, резервное энергоснабжение, аппаратная криптография и т. п.), и, во-вторых, специфические дополнения - межсетевые экраны (firewalls) для защиты каналов Интернета. Такой подход позволяет использовать единые методики оценки рисков при проведении электронных платежей вне зависимости от способа аутентификации клиента (традиционная карта с магнитной полосой, смарт-карта или цифровой сертификат). Это позволяет участникам платежной системы разрешать спорные ситуации по отработанным механизмам и сконцентрироваться на развитии своего электронного бизнеса [1].

SET обеспечивает следующие требования защиты операций в среде электронного бизнеса:

1) секретность данных оплаты и конфиденциальность информации заказа, переданной вместе с данными об оплате;

2) сохранение целостности данных платежей, которая обеспечивается при помощи цифровой подписи;

3) специальную криптографию с открытым ключом для проведения аутентификации;

4) аутентификацию держателя кредитной карты, которая обеспечивается применением цифровой подписи и сертификатов держателя карты;

5) аутентификацию продавца и его возможности принимать платежи по пластиковым картам с применением цифровой подписи и сертификатов продавца;

6) подтверждение того, что банк продавца является действующей организацией, которая может принимать платежи по пластиковым картам через связь с обрабатывающей системой, что обеспечивается с помощью цифровой подписи и сертификатов банка продавца;

7) готовность оплаты транзакций в результате аутентификации сертификата с открытым ключом для всех сторон;

8) безопасность передачи данных посредством использования криптографии.

SET позволяет сохранить существующие отношения между банком, держателями карт и продавцами, и объединяется с действую-

щими системами, опираясь на открытость, международные стандарты платежных систем, лежащие в его основе, а также технологии и правовые механизмы, существующие в финансовой отрасли [1].

Таким образом, выявление предпосылок, тенденций интеграции бизнес-процессов компании в среду электронного бизнеса в условиях российской экономики, научное обобщение опыта зарубежных стран и выработка рекомендаций по использованию и развитию электронного бизнеса в России являются важными народнохозяйственными задачами и требуют решения проблемы обеспечения информационной безопасности при интеграции бизнес-процессов компании в среду электронного бизнеса.

Библиографический список

1. Зайцева Е.В. Основы электронного бизнеса: Учебное пособие для специальности 080503./ Е.В.Зайцева – Томск: кафедра ТУ, ТУСУР, 2012. – 263 с.

2. Нил Бакманн Доклад на конференции "Перспективы использования интернет-технологий в бизнесе", 26 октября 2000 г., Ярославль – Режим доступа: http://www.incap.ru:8101/confprog.htm

Петрова Е.Д.

к. биол. н., профессор кафедры общей психологии

ПСИХОЛОГИЧЕСКИЕ ОСОБЕННОСТИ ЛИЧНОСТИ С ИНТЕРНЕТ-АДДИКЦИЕЙ

ФГБОУ ВПО «Магнитогорский государственный университет»,
inform@masu-inform.ru

Аннотация

В статье отражены результаты, полученные в ходе проведенного эмпирического исследования по изучению личностных особенностей лиц с Интернет-аддикцией. Установлено, что для Интернет-аддиктов характерны повышенная сензитивность и тревожность, слабая значимость активных социальных контактов и семейной жизни, чувство одиночества в реальной жизни, внутренний конфликт между стремлением к людям и их избегание, представление об Интернете как об реальности.

Одним из показателей ухудшения психического здоровья людей является стремление все большего количества людей к уходу от реальности путем изменения своего психического состояния посредством наркотиков, алкоголя, никотина или постоянной фиксации внимания на определенных предметах или видах деятельности, что сопровождается развитием интенсивных эмоций.

Современное психологическое знание демонстрирует возрастающий интерес к проблеме Интернет-аддикции, которая является

формой аддиктивного поведения, но при этом не относится к разряду физических зависимостей, а является чисто психологической.

Погружению человека в Сеть способствуют следующие [2, 4]:

– недостаток общения в реальном мире (большая часть Интернет-зависимых использует сеть Интернет ради общения, поскольку виртуальное общение имеет преимущества по сравнению с реальным);

– чувство защищенности в Сети (по данным опросов, Интернет-зависимых привлекают такие особенности Сети, как анонимность, доступность, безопасность и простота использования);

– возможность уйти от реальности (на сегодняшний день можно утверждать, что Интернет стал одним из видов «буферной» реальности, предохраняющей личность от прямого соприкосновения с реальным миром).

Погружение в виртуальную среду может быть обусловлено внутренними психологическими конфликтами, вызванными, например, проблемами в личной и семейной жизни, для детей - трудностями в общении со сверстниками. Погружаясь в виртуальную реальность, человек защищает себя от каких-то проблем, тревоги, комплексов. Виртуальный мир может использоваться как средство компенсации неудач. Именно виртуальный мир дает ту свободу действий, свободу выражения мыслей, чувств и эмоций, которые в реальной жизни зачастую не всегда возможны. Также сетевая зависимость может быть следствием психотравмирующей ситуации (потеря близкого человека, работы, семьи и т.д.)[1].

Аддиктивный подход к разрешению проблемных ситуаций зарождается в глубине психики, он характеризуется установлением эмоциональных отношений, эмоциональных связей не с другими людьми, а с неодушевленным предметом или активностью. Человек нуждается в эмоциональном тепле, интимности, получаемых от других и отдаваемых им [6].

При формировании аддиктивного подхода происходит замена межличностных эмоциональных отношений проекцией эмоций на предметные суррогаты. Лица с аддиктивным поведением стараются реализовать свое стремление к интимности искусственным образом. На сознательном уровне они используют для самозащиты механизм, который называют “мышлением по желанию”. Он заключается в том, что человек, вопреки логике причинно-следственных связей, считает реальным, допускает до себя, до области своих переживаний лишь то, что соответствует его желаниям. Содержание мышления при этом в свою очередь подчинено эмоциям, которые у аддикта также искусственно обеднены [3].

В связи с этим оказывается невозможным или очень трудным убедить человека с развитым аддиктивным поведением в неправильности, опасности его подходов. Разговор с такими людьми происходит в двух плоскостях, которые не соприкасаются друг с другом: логической и эмоциональной. То, что является очевидным в логической плоскости, не влияет на “мышление по желанию” человека с аддиктивным поведением [4].

Для лиц с аддиктивным поведением характерна иллюзия контроля своих аддиктивных реализаций. Аддикты убеждают других, и, прежде всего самих себя, в том, что в любое время они, с одной стороны, могут, прибегая к аддиктивному уходу, снять напряжение, забыть о неприятностях, с другой — при желании прекратить аддиктивную реализацию. Нередко в стратегию аддиктивного поведения включаются защитные проекционные механизмы, когда проблему идентифицируют где угодно — в неудачном браке [5].

Для аддикта типична гедонистическая установка в жизни, то есть стремление к немедленному получению удовольствия любой ценой. Такая установка — это, как правило, продукт неправильного воспитания в детстве либо последствия перенесенных позднее психических травм, либо (что на практике встречается гораздо чаще) компенсаторная реакция психики на разрушительное воздействие ПНС (полиморфный накопленный стресс) [4].

Разумеется, далеко не каждый человек впадает в Интернет-зависимость. К такому поведению склонны люди с особым типом личности, предрасположенные к различным зависимостям.

С целью проверки гипотезы, что у пользователей с Интернет-аддикцией существуют особенности личности, способствующие формированию зависимого поведения было проведено данное исследование. Изучались индивидуально-типологические свойства личности: иерархия терминальных ценностей и сфер жизнедеятельности, субъективное ощущение одиночества и потребность в аффилиации. Данные личностные особенности составляют определенный преморбидный фон, т.е. способствуют формированию аддиктивного поведения личности.

В исследовании принимало участие 112 респондентов, из которых были выделены экспериментальная и контрольная группы по 40 человек (по результатам шкалы Интернет-аддикции А. Жичкиной и теста на определение Интернет-зависимости К. Янг. Диагностика интернет - зависимости проводилась на основе самостоятельно выполняемой аддиктом оценке проведения свободного времени (например, на какие прежде любимые занятия и хобби не остается времени из-за Интернета, или сколько времени расходуется на конкретные виды опосредствованной Интернетом деятельности, или мимо каких жиз-

ненных интересов пришлось пройти в силу увлеченности Интернетом или какие чувства "эмоциональные крючки" сильно привязывают к Интернету).

В таблице 1 отражены социально-демографические характеристики выборки.

Таблица 1

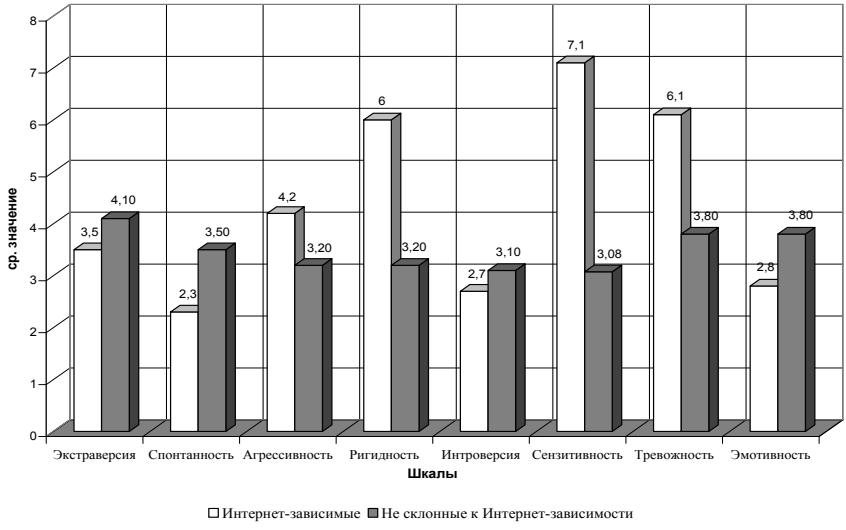
Социально-демографические характеристики экспериментальной и контрольной групп

Характеристики испытуемых	Критерии характеристик испытуемых	Экспериментальная группа (n=40)	Контрольная группа (n=40)	Общая выборка (n=80)
		Чел.	Чел.	Чел.
Возраст	Минимальный	18	18	18
	Максимальный	30	32	32
	Средний	25	25	25
Пол	Женский	8	12	20
	Мужской	32	28	60
Образование	Высшее	27	24	51
	Неполное высшее	8	10	18
	Среднее специальное	4	5	9
	Среднее	1	1	2
Семейное положение	Холост/ незамужем	34	27	61
	Женат/ замужем	6	13	19
Опыт работы в Интернете	Менее 3-х мес.	5	4	9
	От 3-х мес. до 1 г.	7	9	16
	От 1-го г. до 2-х лет	16	6	22
	От 2-х лет до 3-х лет	8	13	21
	Более 3-х лет	4	8	12
Среднее количество времени, проводимо-	1-2 ч. в неделю	-	2	2
	0-30 мин. в день	-	4	4
	30 мин.- 1ч. в	2	3	5

го в Интернете	день			
	1-2 ч. в день	6	18	24
	2-4 ч. в день	8	7	15
	Более 4 ч. в день	24	5	29

В данном исследовании было проведено тестирование с помощью указанных ниже методик, а также математико-статистический анализ полученных данных с помощью t-критерия Стьюдента и коэффициента корреляции Пирсона. Методики исследования: индивидуально-типологический опросник (Собчик Л. Н.); опросник терминальных ценностей (Сенин И. Т.); методика диагностики мотивов аффилиации (Меграбян А.); методика диагностики уровня субъективного ощущения одиночества (Д. Рассела и М. Фергюсон); опросник установок по отношению к Интернету (Дэвис Р., Гордон Л.); методика выявления отношения к Интернету «Незаконченные предложения» (Жичкина А. Е., Щепилина Е. А.); тест на определение Интернет-зависимости (К. Янг); шкала Интернет-зависимости (А. Е. Жичкина).

В ходе проведенного эмпирического исследования были исследованы личностные особенности склонных к Интернет-аддикции



пользователей.

Рис.1. Показатели индивидуально-типологических особенностей личности в экспериментальной и контрольной группах

По методике «Индивидуально-типологический опросник» установлено, что респонденты экспериментальной группы более тревожны, ригидны, сензитивны, менее спонтанны и эмотивны, проявляют конфликтность и конформность по сравнению с респондентами контрольной группы.

При изучении терминальных ценностей было установлено следующее:

1. Наименее значимой ценностью в жизни индивида, склонного к Интернет-аддикции является активные социальные контакты, т.е. для данной личности не свойственно стремление к установлению благоприятных взаимоотношений с другими людьми.

2. Менее незначимой ценностью для Интернет-зависимой личности является креативность, для них не свойственно стремление избегать стереотипов, такие люди предпочитают размеренный ход жизни и не поощряют новшества в своей жизни.

3. Мало значимой сферой жизни Интернет-зависимой личности по результатам исследования является семейная жизнь. Человек пренебрегает проблемами в семейной жизни, тратит на семью, на ее благополучие минимум времени и не интересуется ее развитием.

4. Наиболее значимой сферой жизни Интернет-аддикта можно назвать сферу увлечений. Данные люди считают, что без увлечения жизнь человека во многом неполноценна.

5. Для группы Интернет-независимых по средним значениям, полученным по данной методике можно выделить наиболее значимую сферу жизни – профессиональную жизнь, т.е. такие люди отдают много времени своей работе, включаются в решение всех производственных проблем, считают, что профессиональная деятельность является главным содержанием жизни человека.

6. Преобладающей ценностью Интернет-независимых личностей является высокое материальное положение, т.е. выражается стремление к возможно более высокому уровню своего материального благосостояния. Основанием для развития чувства собственной значимости является высокий уровень материального благополучия.

Полученные результаты по методике «Опросник терминальных ценностей» свидетельствуют, что у респондентов экспериментальной группы наименее значимыми ценностями являются креативность и активные социальные контакты, а наименее значимой жизненной сферой является семейная. В контрольной группе преобладающей ценностью является высокое материальное положение, а наиболее значимой жизненной сферой – профессиональная жизнь.

Таблица 2

Результаты тестирования по методике «Опросник терминальных ценностей»

Показатели	Экспериментальная группа (баллы)	Контрольная группа (баллы)	Достоверность различий (t-критерий Стьюдента)
Терминальные ценности			
Собственный престиж	6,00 ± 0,.29	7,00 ± 0,28	2,49 (p ≤0,05)
Высокое материальное положение	5,20 ± 0,20	8,00 ± 0,26	8,57 (p ≤0,01)
Креативность	3,98 ± 0,33	6,00 ± 0,27	4,78 (p ≤0,01)
Активные социальные контакты	3,18 ± 0.18	6,10 ± 0,27	8,93 (p ≤0,01)
Развитие себя	5,30 ± 0,27	5,15 ± 0,21	
Достижения	5,45 ± 0,25	5,75 ± 0,19	
Духовное удовлетворение	5,48 ± 0,32	5,78 ± 0,28	
Сохранение собственной индивидуальности	5,65 ± 0,25	5,48 ± 0,27	
Жизненные сферы			
Профессиональной жизнь	6,50 ± 0,25	7,15 ± 0,28	
Обучение и образование	4,03 ± 0,17	5,63 ± 0,25	5,37 (p ≤0,01)
Семейная жизнь	3,00 ± 0,18	6,03 ± 0,24	10,06 (p ≤0,01)
Общественная жизнь	5,50 ± 0,27	7,23 ± 0,27	4,52 (p ≤0,01)
Увлечения	8,00 ± 0,22	4,85 ± 0,.29	8,69 (p ≤0,01)

Испытуемые экспериментальной группы чаще испытывают

чувство одиночества в реальной жизни, социальные связи чаще всего устанавливаются посредством Интернет, сеть часто используется как средство избегания выполнения более важных и ответственных дел. Испытуемые контрольной группы способны контролировать время нахождения в сети, у них отсутствуют навязчивые мысли об Интернете, социальные связи устанавливаются в реальной жизни.

По методике «Диагностика уровня субъективного ощущения одиночества» установлено, что склонные к Интернет-аддикции пользователи имеют более высокий уровень субъективного ощущения одиночества. Будучи даже окруженными большим количеством людей, чувствуют себя покинутыми и непонятыми. Не склонные к Интернет-зависимости пользователи более тесно общаются с окружающими и не чувствуют себя одинокими.

По результатам методики «Диагностика мотивов аффилиации» можно судить, что у респондентов экспериментальной группы существует сильно выраженный внутренний конфликт между стремлением к людям и их избеганием. В контрольной группе респонденты активно ищут контактов и общения с людьми, испытывая от этого в основном положительные эмоции.

При качественном анализе полученных данных по методике выявления отношения к Интернету «Незаконченные предложения» выявлено следующее: наиболее часто встречающимися понятиями в экспериментальной группе стали: «сеть», «жизнь», «пространство».

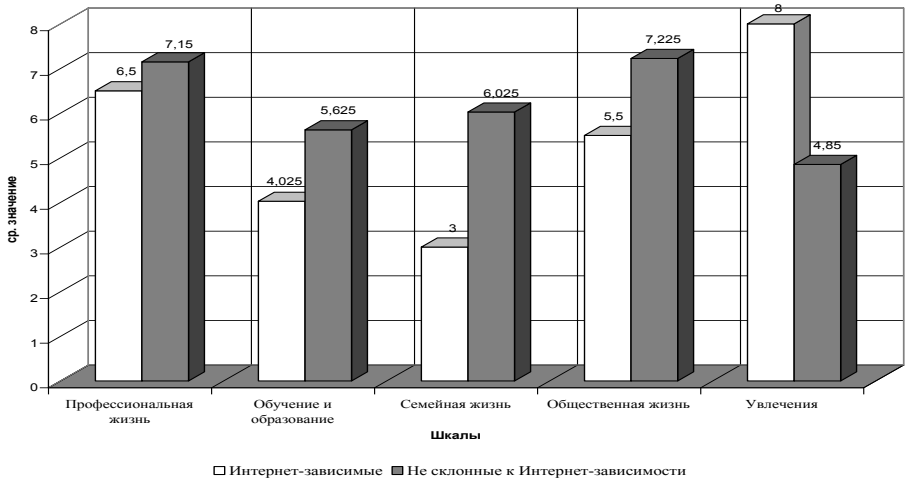


Рис.2. Результаты по методике «Опросник терминальных ценностей»

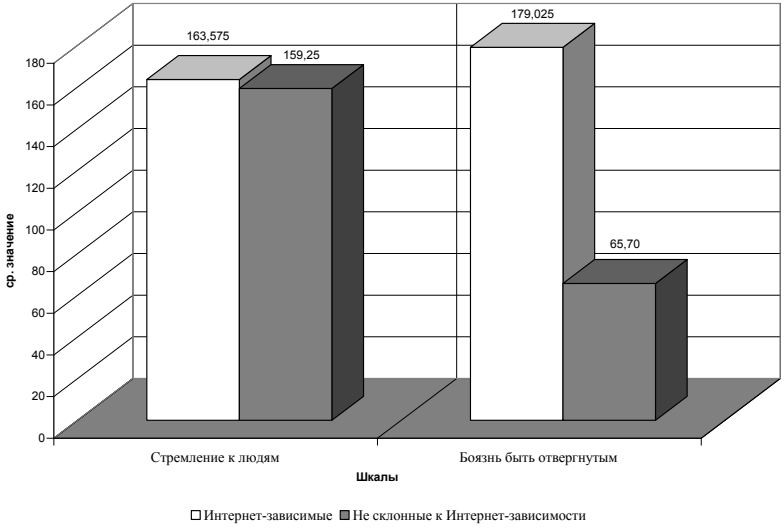


Рис. 3. Показатели по методике «Диагностика мотивов аффилиации»

Эти понятия свидетельствуют о достаточно высокой значимости Интернета в жизни респондентов. Интернет они часто характеризуют в понятиях «лабиринт», «виртуальный мир», «реальность», т.е. он имеет весьма размытые границы, представляет собой отдельную реальность, время в которой течет быстрее, чем в реальном мире. Так-

же отмечается притягательность этого мира, увлеченность им, хотя и признается необходимость сократить время пребывания в сети.

Большая часть испытуемых экспериментальной группы признают, что и в реальной жизни используют сетевой лексикон, иногда стремятся перенести способы поведения из сети в реальность. Находясь в сети, они не всегда могут указать все, где в ней находились, часто отвлекаются на сопутствующую информацию. Некоторые испытуемые отметили, что ощущают «уход в другую реальность», преимущества виртуального общения перед реальным: анонимность, безопасность, возможность одновременно общаться с большим количеством различных людей. Многие отмечают усталость и ухудшение настроения после выхода из сети.

В контрольной группе частыми понятиями являются: «общение», «информация», «игра», «почта», что свидетельствует о низкой персонификации сети для данной категории пользователей. Для этих респондентов характерно отношение к Интернету как к трехмерному пространству, имеющему свои законы, с существующими четкими границами этого пространства.

Испытуемые в контрольной группе не относит себя к сетевой субкультуре, не употребляют сетевой лексикон в своей реальной жизни. Способы их поведения в сети не переносятся в реальный мир. Большинство из них четко знают, зачем они заходят в Интернет, т.е. ставят конкретные цели. Находясь в сети, они не отвлекаются на сопутствующую информацию (объявления, рекламу, баннеры и т.п.). Испытуемые всегда могут вспомнить, где (на каких сайтах) они были, и что там делали. Основной причиной нахождения в сети для них является поиск информации.

Интернет для них всегда остается техническим устройством, пусть даже с почти неограниченными возможностями. Реальное общение является более предпочтительным по сравнению с виртуальным. Интернет не является панацеей от реальных проблем и комфорт в реальной жизни ценится больше комфорта в сети. Настроение до, во время и после выхода из сети остается неизменным, лишь немногие отмечают наличие некоторой усталости.

Таким образом, для испытуемых экспериментальной группы Интернет имеет весьма размытые границы и представляет собой отдельную реальность. Респонденты контрольной группы воспринимают Интернет как средство получения информации, а не как некую реальность.

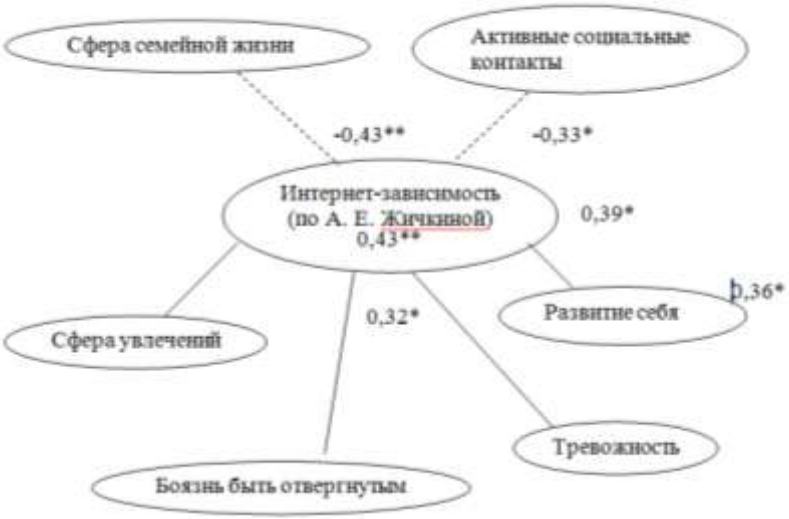


*Рис. 4. Корреляционные связи между интернет-зависимостью (по А. Е. Жичкиной) и шкалами методик в экспериментальной группе интернет-зависимых лиц $p \leq 0,05$ - *; $p \leq 0,01$ - ***

Корреляционный анализ показал, что уровень Интернет-аддикции определяется значимостью сферы увлечений, высокой тревожностью, субъективным ощущением одиночества, ригидностью и боязнью быть отвергнутым, низким значением сферы семейной жизни и ценности активных социальных контактов.

Итак, обобщая полученные результаты нашего исследования можно отметить, что для лиц с Интернет-аддикцией характерны:

1. Повышенная сензитивность и тревожность;
2. Слабая значимость ценности активных социальных контактов и сферы семейной жизни;
3. Высокий уровень субъективного ощущения одиночества, чувство одиночества в реальной жизни;
4. Сильно выраженный внутренний конфликт между стремлением к людям и их избеганием;
5. Представление об Интернете как об отдельной реальности с весьма размытыми границами.

Психопрофилактическая и коррекционная деятельность с интернет-аддикцией ведется различными путями, но наиболее продуктивным способом на сегодняшний день является когнитивно-

бихевиоральная психотерапия. Одной из наиболее серьезных проблем для Интернет-аддиктов является неспособность контролировать время, отдаваемое увлечению. Основное внимание в своей работе психолог должен уделять повышению самоконтроля человека и его самопознанию. Данную работу можно проводить в виде тренингов с элементами коррекции отдельных личностных особенностей и форм поведения, в частности, снижение агрессивности, развитие коммуникативных навыков, повышение самооценки и самоосведомленности, увеличение стабильности межличностных взаимоотношений, повышение социальной адаптации.

Библиографический список

1. Арестова О. Н., Бабанин Л. Н., Войскунский А. Е. Мотивация пользователей Интернета. http://www.relarn.ru:8082/human/motivation.txt.
2. Асмолов, А. Г. Психологическая модель Интернет-зависимости личности / Асмолов А. Г., Цветкова Н. А., Цветков А. В. // Мир психологии. — 2004. — N 1. — С. 179-192.
3. Белинская Е. П., Жичкина А. Е. Стратегии самопрезентации в Интернет и их связь с реальной идентичностью //http://flogiston.ru/projects/articles/strategy.shtml.
4. Войскунский А. Е. Психологические исследования феномена интернет-аддикции //http:// psycom.net.
5. Шевченко И. С. - Некоторые психологические особенности общения посредством Internet //http://www.flogiston.ru.
6. Янг К. Пойманные в сеть //www.netaddiktion.com.

Повитухин С. А.
к. т. н., доцент кафедры информатики

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ДОСТУПА К ДАННЫМ СУБД FIREBIRD

ФГБОУ ВПО «Магнитогорский государственный университет», inform@masu-inform.ru

Аннотация

Обычно БД обслуживаются людьми, некоторые из которых имеют полный доступ к системе, где работает СУБД Firebird и находятся БД. Разработчик, создавая БД и сопутствующее клиентское программное обеспечение должен подумать о защите информации. Для обеспечения безопасного доступа к данным необходимо обеспечить их защиту от несанкционированного доступа, как на уровне сервера, так и на уровне клиента. Данная статья рассматривает аспекты обеспечения безопасности данных при работе с сервером БД Firebird.

Современные сети обеспечивают доступ к одним и тем же файлам сразу для нескольких пользователей. Таким образом становиться возможным доступ к одному файлу (файлам) БД с помощью нескольких приложений. Подобную архитектуру называют файл–серверной.

С её помощью возможно построение многопользовательской информационной системы. Однако такая архитектура имеет существенный недостаток: обработка происходит на рабочем (локальном) компьютере, в результате чего резко повышается нагрузка на сеть.

При использовании архитектуры клиент–сервер доступ к файлам данных имеет только сервер БД. Сервер БД – специальная программа, обслуживающая запросы клиентских программ, запущенных на рабочих компьютерах. При подключении к БД пользователю нет необходимости иметь прямой доступ к файлу (файлам) БД. Все соединения и весь доступ происходит через сервер БД, который выполняет обращение к БД по необходимости. Клиент формирует запрос к серверу на языке запросов SQL, являющимся промышленным стандартом для реляционных БД. При этом запросы пользователя обрабатываются не на рабочем компьютере, а на сервере БД. SQL–сервер оптимизирует

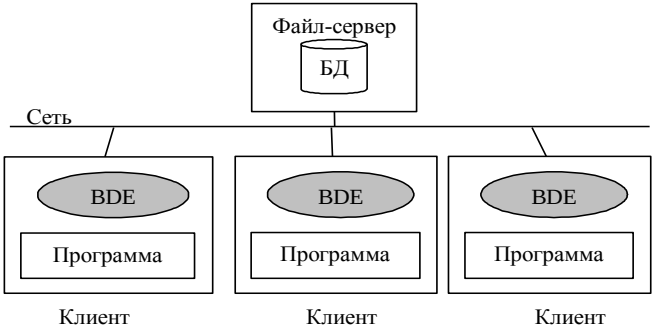


Рис. 1. Архитектура файл\сервер

запрос, с целью уменьшения времени выполнения, и возвращает клиенту результаты запроса. Сервер при этом является тем «устройством», которое обеспечивает доступ зарегистрированным пользователям в соответствии с правами этих пользователей.

В случае использования клиент–серверной архитектуры с помощью Delphi или другой системы программирования создаются 2- или 3- уровневые приложения. При создании 2- уровневых приложе-

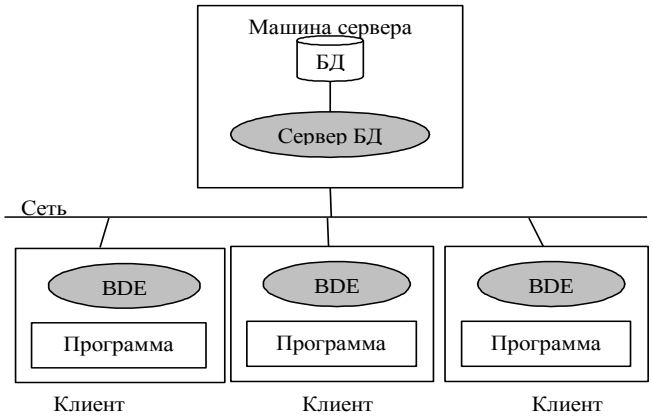


Рис. 2. 2-х уровневая архитетура клиент\сервер.
«Толстый» клиент.

ний создается только «толстый» клиент, который обращается к какому-нибудь промышленному SQL–серверу.

Для получения доступа к БД, приложению (пользователю) необходимо подключиться к процессу сервера БД, например Interbase или его бесплатному аналогу Firebird. СУБД Firebird в 2010 году отметила свое десятилетие. СУБД Firebird построена на базе кода InterBase, открытого в 2000 году, поэтому общий «возраст» Firebird можно считать равным примерно 25 лет. В настоящее время Firebird успел распространиться очень широко. Его применяют в самых разнообразных системах – начиная от движка доступа к данным для справочных систем, распространяемых на компакт-дисках, до ERP-систем, обрабатывающих сотни гигабайт данных, и обслуживающих сотни пользователей.

При выборе СУБД следует в первую очередь определиться с двумя основными критериями, влияющими на эффективность их использования в качестве эффективного хранилища данных: количество одновременно работающих пользователей и объем ежедневно вносимой в базу данных информации. В терминах СУБД эти критерии относятся соответственно:

- к механизму реализации «блокировок», обеспечивающий гарантию целостности данных при многопользовательском режиме доступа. При этом предпочтение следует отдавать СУБД, которые не блокируют соседние записи при вставке и изменении данных.

• к механизму «секционирования» данных для уровня изоляции транзакций «read–commited». Механизм позволяет разделять большие (критичные по объему) БД, таблицы и индексы на множество мелких управляемых частей, каждая из который может быть доступна более эффективным способом, чем весь массив данных в целом.

• к механизму транзакций, под которым понимается группа операций обработки данных, выполняемых как неделимое действие над БД. При этом запись данных в БД производится только при успешном выполнении всех операций группы (либо все, либо ничего). Если хоть одна операция из группы завершается неуспешно, то БД возвращается к исходному состоянию, в котором она была до начала транзакции. Каждая транзакция реализует некоторую прикладную функцию, например перевод денег с одного счета на другой (операция снятия денег с одного счета и внесения их на другой счет). Такая операция должна составлять единую транзакцию. Иначе может возникнуть ситуация, когда первый SQL–оператор переведет деньги на другой счет, а второй, выполняющий снятие их со счета, не доведет дело до конца из–за непредвиденного сбоя.

СУБД Firebird является высокопроизводительной кросс–платформенной реляционной БД, сочетающей простую инсталляцию, низке системные требования и минимальную потребность в сопровождении. Система работает на Linux, Microsoft Windows и разнообразных Unix платформах. В отличие от большинства современных СУБД, Firebird разработана с целью уменьшения затрат на сопровождение. Мощность, простота использования, бесплатность, поддержка различных платформ (Windows, Linux и Solaris), выводят Firebird в фавориты среди разработчиков и делают ее наиболее приемлемым решением среди корпораций. Одними из главных особенностей СУБД Firebird является: версионная архитектура, наличие обработчиков оповещений о событиях, хранимых процедур, триггеров, генераторов, полный контроль за транзакциями, резервное копирование на лету, наличие определяемых пользователем функций (UDF) и фильтров для работы с объектами BLOB.

В современных ИС важно не только правильно спроектировать структуру БД и манипулировать данными, но также и обеспечить защиту этих данных. Защита данных - это мероприятия по охране данных от множества возможных угрожающих ситуаций, как преднамеренных, так и случайных. Безопасность сервера Firebird исходит из предположения о том, что серверный процесс будет работать в безопасном окружении. Сама СУБД Firebird не предпринимает никаких мер для обеспечения внешней безопасности. Единственный способ обеспечения эффективных мер безопасности заключается в том, чтобы

серверное оборудование было установлено в месте, с ограничением физического доступа посторонних лиц.

В системе имеется пользователь, администратор СУБД, с именем SYSDBA, и имеющий неограниченный доступ ко всем БД, доступным установленной СУБД. Учетная запись SYSDBA используется для настройки привилегий в соответствии с определенными пользователями и требованиями сервера. Причем права, определенные в конкретной БД, игнорируются, если подключение к БД осуществляется пользователем SYSDBA. Если некто, под именем SYSDBA, получает физический доступ к СУБД, то не существует способов предотвратить доступ ко всем данным файлов БД. Это означает, что если у кого-то есть прямой доступ к файлу БД, то он без труда сможет скопировать этот файл с сервера, где пароль пользователя SYSDBA неизвестен, на другой сервер, где пароль будет известен и получит, таким образом, неограниченный доступ к содержимому БД. Следовательно, файлы БД никогда не следует располагать в папках, к которым открыт доступ из сети или доступ любых локальных пользователей, кроме специально оговоренного персонала. Защита данных или метаданных БД возможна только при сохранении контроля над файлом БД и над окружением, в котором происходит работа с этим файлом. Никакое другое решение не обеспечит такой же уровень безопасности.

Следующим уровнем обеспечения безопасности является ограничение прав пользователей на сервере. Здесь рассматривается система управления доступом к данным и механизм транзакций, принятые в языке SQL. Схема доступа к данным в реляционных СУБД базируется на следующих основных принципах:

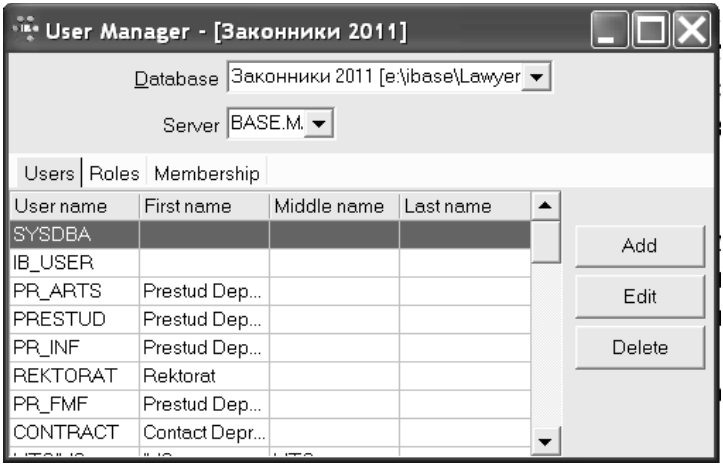


Рис. 3. Регистрация пользователей

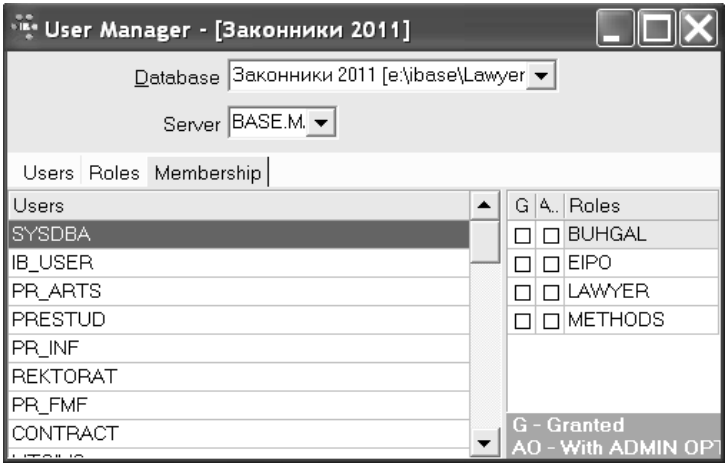


Рис. 4. Назначение ролей пользователям

1) **Пользователи**. Пользователи рассматриваются как основные действующие лица СУБД, желающие получить доступ к данным. Пользователь – это регистрационная (учетная) запись, доступная во всех БД, обслуживаемых сервером. Создание учетной записи пользователя само по себе не дает ему никаких прав на доступ (привилегии) к объектам БД. Чтобы зарегистрировать нового пользо-

вателя, необходимо воспользоваться инструментом администрирования БД, например, бесплатное ПО IBExpert, выбрав в нем пункт «Менеджер пользователей» меню «Инструменты».

2) **Объекты доступа.** Объекты доступа это элементы БД, доступом к которым можно управлять (назначать права доступа конкретному пользователю к конкретному объекту БД). Обычно объектами доступа являются таблицы, однако ими могут быть и другие объекты БД – представления, хранимые процедуры и т.д. Первоначально только создатель объекта БД имеет к нему доступ, и только он может передать определенные привилегии доступа другим пользователям или хранимым процедурам. Если доступ пользователя к объекту не разрешен, то он не может к нему обратиться.

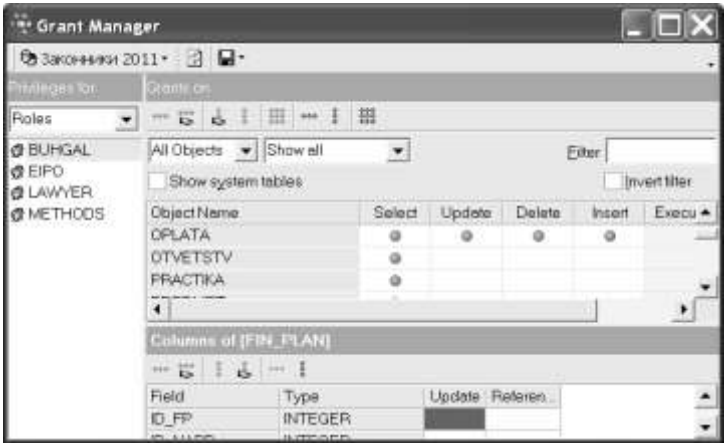


Рис. 5. Предоставление прав доступа

3) **Привилегии.** Привилегии – это системный признак, определяющий операции, которые разрешено выполнять пользователю над конкретными объектами. Все объекты БД имеют определенный уровень доступа при их создании. Далее СУБД будет выполнять операции над объектами БД от имени конкретного пользователя. Она делает это в зависимости от того, обладает ли конкретный пользователь правами на выполнение конкретных операций над конкретным объектом БД. Например, пользователь может добавлять строки в таблицы (INSERT), удаляет строки (DELETE), обновляет данные в строках таблицы (UPDATE). Причем различные объекты имеют различные привилегии. Следует отметить, что СУБД не проверяет никакие права доступа для пользователя SYSDBA – администратора БД. Установление и контроль привилегий являются его обязанностью.

4) **Роли**. Роль представляет собой метод обеспечения безопасности на уровне групп привилегий. Можно сказать, что роль выступает в качестве объекта БД, концентрирующего в себе заданные привилегии доступа к определенным объектам БД. Концепцию планирования безопасности можно представить следующим образом: администратор SYSDBA в соответствии с информационной моделью создает БД. Затем с помощью запроса GRANT передает привилегии определенным пользователям в соответствии с их уровнем доступа к данным, а при подключении к БД пользователь, обладающий какой–либо ролью (ролями), должен указать имя этой роли. При получении запроса на соединение процесс сервера удостоверяет пользователя по БД. Если удостоверение прав пользователя прошло успешно, то сервер разрешает произвести доступ к БД. При этом сервер использует роли и права пользователей, определенные в самой БД. Они обеспечивают «тонкую» настройку системы доступа к объектам БД.

Сервер Firebird поддерживает множество способов доступа, включая: собственные наборы компонент для C/C++, Delphi, классы для ADO, ODBC, JDBC (Jaybird), драйверы для Python, PHP, драйвер OLE DB, dbExpress, провайдер данных .NET и прямой доступ с использованием клиентской библиотеки сервера (fbclient.dll или GDS32.dll). При этом так же по различных причинам возможно разрушение или порча данных:

- порча или изменение данных анонимным пользователем;
- завершение работы программ при системном сбое, когда база данных остается в непредсказуемом состоянии;
- возникновение конфликта при выполнении двух и более программ, конкурирующих за одни и те же данные;
- изменение базы данных недопустимым способом обновления и т.д.

Драйвер dbExpress фирмы Borland предлагает новый подход к предоставлению общего API для разных БД с технологией Borland provider/resolver для управления работой с данными. В этой статье рассматривается архитектура dbExpress и механизм provider/resolver на примере создания приложения основанного на использовании компонент dbExpress.

Архитектура provider/resolver использует четыре типа компонент для предоставления данных с сервера, их редактирования и сохранения:

1) SQLConnection – предназначен для установления соединения между драйвером dbExpress и используемым сервером БД;

2) Компоненты, предоставляющие доступ к данным, получаемым оператором SELECT или вызовом хранимых процедур, например, TSQLClientDataSet;Компонент DataSetProvider, открывающий

компонент, выполняющий запрос или хранимую процедуру и закрывающий этот компонент после поставки данных;

3) Компонент ClientDataSet, запрашивающий полученные данные у DataSetProvider.

На рисунке 6 приведен пример модуля данных для клиента БД, реализованный в Delphi 6.0.

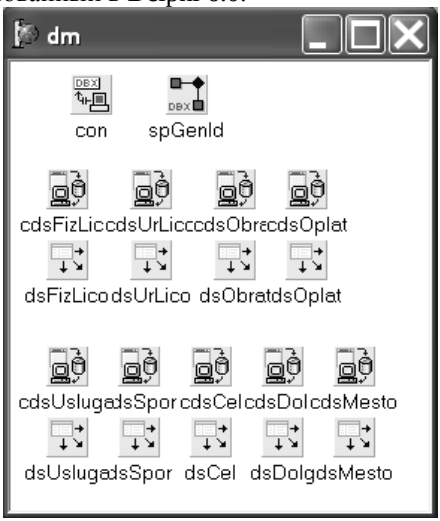


Рис. 6. Модуль данных

Подключение к БД должно выполняться при запуске приложения пользователем, который должен вводить свое имя и роль. В противном случае, если подключение было выполнено на этапе разработки, пароль будет сохранен в программном коде и, следовательно, возможен несанкционированный доступ к данным.

Одним из вариантов решения проблемы является подключение к серверу с использованием ini–файла, в котором записаны параметры подключения, кроме пароля. Это позволяет легко настраивать параметры на различных рабочих местах. Для загрузки параметров из файла необходимо добавить следующий код в событие DataModuleCreate:

```
con.LoadParamsFromIniFile('Centr.ini');
con.Connected:=true
```

DriverName=Interbase
BlobSize=-1
CommitRetain=False
Database=<путь к БД>\<имя БД>.gdb
ErrorResourceFile=
LocaleCode=0000
Password=
RoleName=operator
ServerCharSet=win1251
SQLDialect=3
Interbase TransIsolation=ReadCommited
User_Name=oper
WaitOnLocks=True

Рис. 7. Пример ini-файла

Пример ini–файла приведен на рис. 7. При запуске приложения отображается стандартное окно регистрации, в котором пользователь вводит свое имя и пароль для доступа к серверу. Роль, назначенная пользователю, указана в параметре RoleName.

Библиографический список

1. Ковязин А., Востриков С. Мир Interbase. Архитектура, администрирование и разработка приложений баз данных в Interbase/Firebird/Yaffil – М.: КУДИЦ-ОБРАЗ, 2002. – 432 с.
2. Джеймс Р. Грофф, Пол Н. Вайберг. SQL: полное руководство: пер. с англ. – К.: Издательская группа BHV, 1999. – 608 с.
3. Дейт Дж. К. Введение в системы баз данных. – 8–е изд. М.: Вильямс, 2006. 1328 с.
4. Тексейра Стив, Пачеко Ксавье. Delphi 4. Руководство разработчика.: Пер. с англ. – К.; М.; СПб.: Издательский дом «Вильямс», 1999.
5. Хомоненко А.Д., Гофман В.Э. Работа с базами данных в Delphi. – СПб.: БХВ – Петербург. – 2005. 535 с.
6. http://www.ibase.ru/devinfo/dbexpress.htm
7. http://www.firebirdsql.org/manual/ru/fbmetasecur-ru.html#fbmetasecur-intro-ru

Ращупкин А.А.,
студент факультета информатики

ПРИМЕНЕНИЕ МЕТОДА ПРОЕКТОВ ПРИ ПОДГОТОВКЕ ШКОЛЬНИКОВ К ЗАЩИТЕ ОТ КИБЕРПРЕСТУПЛЕНИЙ

ФГБОУ ВПО «Магнитогорский государственный университет»,
shamanx74@gmail.com

Аннотация

Статья раскрывает суть учебного проекта, призванного обратить внимание старшеклассников на участившиеся случаи киберпреступности, рассмотреть способы защиты информации от киберпреступников.

В век информационного общества компьютерные преступления и телекоммуникационные системы стали играть огромную роль в деятельности людей и государства. Но люди не предполагали, что со временем Интернет для них окажется объектом злоупотребления и причиной всех бед, органом по вопросам расследования таких преступлений. Рассматривая один из видов мошенничества в сети – киберпреступления, можно прийти к выводу, что сегодня – это очень выгодный и процветающий бизнес. В современном обществе преступник, занимающийся незаконной деятельностью, согласно обзорам авторитетных зарубежных издательств, зарабатывает в среднем несколько миллиардов долларов в год [1].

Понятие киберпреступности имеет международное значение и означает совершаемые людьми преступления, в процессе которых информационные технологии используются в преступных целях. Уровень развития этого вида преступлений зависит от многих факторов, от степени развитости информационных технологий и глобальных сетей, а также от открытости доступа к ним.

Различают четыре вида компьютерных преступлений – спаминг, кардинг, фишинг и бот-сети.

В основе спаминга лежит рассылка незапрашиваемых массовых сообщений по электронной почте. При этом в рассылаемое сообщение входит рекламный текст или иное нежелательное содержимое.

Под кардингом имеют в виду разного рода махинации с банковскими картами – в них незаконно используются сами карты или информация о них.

Фишинг – это преступление, в котором все персональны данные о картах и счетах клиента добывается злоупотреблением доверием (мошенничеством) – всю требуемую информацию владельцы карт передают преступникам добровольно. Часто фишинг осуществляется рассылкой по электронной почте официального письма якобы от имени представителя банка.

Ну и наконец, бот-сети представляют из себя сети в Интернет зомбированных (инфицированных) компьютеров. Зараженный компьютер-бот в дальнейшем используется для рассылки спама, проведения атак на отказ в обслуживании, организации клик-фрода.

Спамеры, хакеры, кардеры, фишеры и им подобные – все это названия определяющие людей, занимающихся киберпреступлениями. Если ранее деятельность этих преступников распространялась только на корпоративных клиентов, то на данное время их вред касается и рядовых граждан [2] .

К числу их преступлений можно отнести взлом паролей, распространение вредоносных программ, рассылка спама, кражи информации, касающейся любой деятельности человека, распространение клеветы, порнографии, материалов, которые могут повлечь межрелигиозную или национальную вражду.

Пользователи становятся заложниками групп преступников и мошенников из-за своей халатности. Многие либо ленятся, либо не знают, как можно защитить и сохранить свои данные. А ведь это – основная причина всех бед.

Именно поэтому количество преступлений неизменно растет. В России самыми популярными среди киберпреступлений является воровство денег с банковских счетов пользователей сети Интернет. Как действуют преступники: мошенник заражает компьютер жертвы специальным вирусом, через него устанавливается удаленный доступ. Когда человек заходит на свой банковский счет, преступник в это время незаметно переводит деньги на подставные счета[3].

Другим популярным способом является так называемая фишинговая атака. Действует она таким образом: пользователь получает письмо якобы от своего банка с просьбой зайти на счет и поменять информацию. Ссылка из этого письма ведет на сайт-подделку, который полностью копирует банковский сайт. Пользователь переходит на этот сайт, вводит там свой логин и пароль от своего счета и попадает в ловушку мошенников, сам не замечая того – все данные, которые пользователь вводил на сайте – пересылаются злоумышленникам.

В сети необходимо проявлять бдительность, не переходить по сомнительным ссылкам, не посещать малоизвестные и непроверенные сайты, а самое главное – перепроверять все связанное с деньгами. Вирусы чаще всего проникают на компьютер вместе с программой, которая обещает пользователю что-то бесплатное, если он ее установит. В этом случае перед установкой любой программы ее необходимо проверить антивирусной программой. Только после этого можно быть уверенным, что данные, находящиеся у вас на компьютере, не попадут в чужие руки.

Актуальность исследования обусловлена необходимостью в защите от компьютерных преступлений. Школьники проводят за компьютером очень много времени, но при этом они часто забывают об основных правилах безопасной работы в Интернете. Именно из-за этого и происходит утечка информации.

Цель проекта – обратить внимание на участившиеся случаи киберпреступности, рассмотреть способы защиты информации от киберпреступников.

В соответствии с целью и предметом исследования были определены следующие задачи:

1. Уточнить сущность и содержание понятия компьютерное преступление.
2. Выяснить, кто такие киберпреступники, как они действуют и какую опасность представляют для данных.
3. Рассмотреть всевозможные методы защиты от кибепреступников.
4. Предложить учащимся подготовить доклады на заданные темы.
5. Провести анализ знаний учащихся по теме «Компьютерные преступления» при помощи итогового тестирования.

Мероприятие, посвященное компьютерным преступлениям, состоит из теоретического и практического этапа. На первом этапе преподаватель проводит лекцию, где рассказывает о компьютерных преступлениях. После окончания лекции учащимся предлагается выбрать несколько тем, после чего представить их в виде доклада – презентации. На втором этапе преподаватель, дабы проверить, как учащиеся усвоили материал, предлагает пройти тест, состоящий из 15-ти вопросов.

Общеизвестно, что тестирование является наиболее объективным измерителем качества обучения. Контроль в форме тестирования дает возможность проверить учащихся по большому объему изучаемого материала и получить объективное представление о системе его знаний. Такой контроль обеспечивает самую эффективную обратную связь.

После проведения тестирования подводятся итоги проекта. Учащиеся получают сертификаты, в которых указываются фамилии и имена участников, название мероприятия и набранные баллы за тестирование и доклады.

Пропагандировать защиту от киберпреступлений можно через целый ряд мероприятий в виде лекций, презентаций, деловых игр и практической работы – тестирования, ведь учащиеся должны не только хорошо разбираться в компьютерных преступлениях, знать все виды кибепреступлений и отличать, например, хакера от кардера, но и

уметь защищать свою информацию от киберпреступников.

Осведомленность и знания учащихся о защите от компьютерных преступлений – это первый шаг к тому, чтобы избежать опасности и защитить свои данные.

Публикация выполнена при поддержке гранта РГНФ № 13-06-00156 «Подготовка педагогических кадров к профилактике и противодействию идеологии киберэкстремизма среди молодежи»

Библиографический список

1. Киберпреступления по своим масштабам не уступают контрабанде наркотиков. [статья]. URL: http://sitestroyblog.ru/kiberprestupleniya-po-svoim-masshtabam-ne-ustupayut-kontrabande-narkotikov/ (дата обращения: 25.12.2012)
2. Кредитные карты. Ассоциация региональных банков России. [статья]. URL: http://www.asros.ru/ru/financial/fin5/ (дата обращения: 17.01.2013)
3. Статистика киберпреступлений за 2012 год. [доклад]. URL: http://www.businesslynch.ru/2013/02/2012.html (дата обращения: 12.12.2012)
4. Метод проектов [статья]. URL: http://courses.urc.ac.ru/eng/u6-3.html (дата обращения: 24.11.2012)

Савельева Л.А.
к.п.н., доц. каф. прикладной информатики
Мартынюк А.В.
студент факультета информатики

ВОПРОСЫ ФОРМИРОВАНИЯ СОЦИАЛЬНО-ПРАВОВОЙ КОМПЕТЕНЦИИ УЧАЩИХСЯ НА УРОКАХ ИНФОРМАТИКИ

ФГБОУ ВПО «Магнитогорский государственный университет», Sla4@mail.ru

Аннотация

В статье пойдет речь о компетенции, информационной компетенции и в частности о социально-правовой компетенции на уроках информатики, которая предполагает овладение учащимися комплексом универсальных правовых действий, взаимосвязь личностных и социально-ценностных качеств, а также о компетентностном подходе, объединяющем в себе интеллектуальные и навыковые составляющие образования.

В настоящий момент можно наблюдать очередной этап технологической революции — становление информационного общества. Новые реалии ставят перед образованием новую проблему — подгото-

вить современного человека к жизни и деятельности в быстро меняющемся информационном обществе, в мире, где ускоряется процесс появления новых знаний, постоянно возникает потребность в новых профессиях, непрерывном повышении квалификации.

Для того чтобы быть успешным в современном обществе человек должен обладать высоким уровнем информационной компетентности, которая подразумевает:

- умение грамотно формулировать свои информационные потребности и запросы;
- работать с различными источниками информации, находить и выбирать необходимый материал, классифицировать его, обобщать, критически к нему относиться;
- эффективно использовать компьютерные и телекоммуникационные технологии;
- на основе полученного знания конкретно и эффективно решать какую-либо информационную проблему.

Информационная компетентность понимается как интегрированное качество личности, представляющее собой единство мотивационной теоретической и практической готовности и способности школьника к осуществлению информационной деятельности, основанной на усвоении способов приобретения знаний из различных источников информации.

Компетенция – открытая система знаний (процессуальных, ценностно-смысловых, системных, декларативных), которая активизируется и обогащается в деятельности по мере возникновения реальных жизненно важных проблем, с которыми сталкивается носитель компетенции.

Компетентность можно сформировать только на практике. Следовательно, большее внимание со стороны учителя должно уделяться практической направленности учебных материалов и методики формирования социально-правовой компетенции.

Основной базой в изучении методики социальных и педагогических технологий послужили исследования В.П Беспалько, С.А. Беличевой, И.Ф. Дементьевой, И.Г. Зайнышева, З.Я. Капустиной, Л.В. Мардахаева, Г.С. Семенова, В.С. Торохтия, М.В. Шакуровой, Н.Е. Щурковой.

Исследование проблемы правового образования учащихся, с целью формирования социально-правовой компетентности, осуществляются в следующих направлениях:

- • проблемы формирования экономических и правовых знаний как средств обеспечения социальной защищенности учащихся (С.К. Омаров);

- • правового воспитания учащихся (ГА. Дмитриев, Т.В. Корчагина, А.Ф. Никитин, Н.Г. Суворова, Н.И. Элиасберг).

Опираясь на работы А.А. Кузнецова, М.П. Лапчика и др. ученых-педагогов, будем считать, что информационная компетентность представляет собой совокупность следующих компонентов:

- компетенции в сфере информационно-аналитической деятельности;
- компетенции в сфере познавательной деятельности;
- компетенции в сфере коммуникативной деятельности;
- технологические компетенции;
- компетенции в области техникознания (техническая компетенция);
- компетенции в сфере социально-правовой деятельности [2].

Каков идеальный тип человека современности и ближайшего будущего? Это самостоятельный, предприимчивый, ответственный, коммуникабельный, толерантный, способный видеть и решать проблемы автономно, а также в группах, готовый и способный постоянно учиться новому в жизни и на рабочем месте, самостоятельно и при помощи других находить и применять нужную информацию, работать в команде и т.д. Все вышеперечисленные свойства и качества универсальны и необходимы любому человеку в любой профессиональной деятельности.

Необходимость обучения подобным качествам (компетенциям) по существу и является ответом образования на вызовы современного общества, которое характеризуется все возрастающей сложностью и динамизмом. Отсюда и компетентностный подход в обучении сосредоточивается на том, чтобы не увеличивать объем информированности человека в различных предметных областях, а помочь людям самостоятельно решать проблемы в незнакомых ситуациях. Те же умения, которые помогают человеку ориентироваться в новых ситуациях своей профессиональной, личной и общественной жизни, достигая поставленных целей, стали называть компетенциями или ключевыми компетенциями.

В мировой образовательной практике понятие компетентности, как цели образования, выступает в последние годы в качестве одного из центральных понятий. А как основное направление реформирования (или модернизации) школы в образовательные цели школы включены: формирование ключевых компетенций и связанного с этим изменения методов учебной работы. Причин для этого несколько. Основная причина - необходимость усиления ориентации школы на изменившиеся условия жизни современного общества и, в особенности, сферы труда.

Именно компетентностный подход в состоянии, по мнению многих авторов, адекватно ответить на эти требования: во-первых, компетентность объединяет в себе интеллектуальные и навыковые составляющие образования. Эти составляющие выступают в традиционной школе зачастую в несвязанном виде, когда знания сообщаются в отрыве от их применения в практически ситуациях. Во-вторых, в понятии компетентности заложена новая идеология интерпретации содержания образования, формируемого «от результата». В-третьих, ключевая компетентность обладает интегративной природой, так как она вбирает в себя ряд однородных или близкородственных умений и знаний, соответствующих относительно широкой сфере культуры и деятельности (информационной, правовой и т.д.) [4].

В настоящее время не только педагогическое сообщество, но и общество в целом понимает, что владение компьютером (компьютерная грамотность) представляет собой важнейший элемент образования. Значительные средства тратятся на компьютеризацию школ. Однако само понятие «компьютерная компетентность» остается достаточно расплывчатым. Можно ли сказать, что каждый человек, который играет в компьютерные игры, а также пользуется электронной почтой или Интернетом, по-настоящему владеет компьютером? Достаточно ли тех знаний и умений, которые современные молодые люди получают в школе, для решения задач, с которыми они столкнутся в реальной жизни? Исчерпывают ли элементарные навыки работы с текстовым редактором те требования, которые выдвигают современное производство или обучение в высшем учебном заведении?

На все эти вопросы нужно ответить отрицательно. В большинстве школ компьютеры используются просто как современные аналоги традиционных пишущих машинок, калькуляторов или проекторов. Многие их возможности вовсе не используются или используются лишь в минимальном объеме.

В новых публикациях на эту тему, подготовленных педагогическими сообществами, отмечается, что ИКТ могут использоваться в школах более эффективно. Ведущие теоретики и практики демонстрируют, как это можно и нужно делать. Большинство из них придерживаются того мнения, что широко практикуемое обучение изолированным умениям в условиях особых «компьютерных классов» чаще всего не достигает своей цели.

В качестве альтернативы такому методу обучения работе на компьютере они предлагают путь интеграции чисто технических моментов и содержательных задач различного рода. Руководящим принципом тут выступает положение о том, что конечным результатом обучения должно стать не понимание того, как функционирует компьютер, а способность использовать его в качестве инструмента реше-

ния разнообразных задач, коммуникации, организации деятельности, в частности – исследовательской. А это, в свою очередь, влечет за собой существенное изменение общей методики преподавания и конкретных акцентов.

Переход от обучения отдельным навыкам работы на компьютере к интегрированному способу выработки компьютерной компетентности предполагает специальные усилия в этом направлении.

Правильно построенная программа выработки компьютерной компетентности не должна сводиться к простому перечню тех знаний и умений, которыми учащиеся должны овладеть (знание устройства компьютера, навыки работы с текстовым редактором, умение искать и находить нужную информацию в Интернете).

Хотя подобные знания и умения действительно важны, традиционный путь обучения им в изолированном виде не обеспечивает успешного переноса навыков из одной ситуации в другую. Ученики овладевают отдельными приемами работы на компьютере, но у них не возникает понимания того, как эти приемы должны сочетаться между собой для решения разнообразных практических задач. Подлинное владение компьютером предполагает направленное, творческое и гибкое использование этого мощного инструмента.

Учащийся должен хорошо представлять себе конечную цель, понимать, как с помощью компьютера можно решить различные возникающие при этом задачи, и уметь реально использовать различные технические приспособления и возможности. Каждый отдельный навык работы на компьютере, интегрированный в процесс решения практических задач, приобретает для человека совершенно иной личностный смысл [2].

Только в этом случае правомерно говорить о подлинной компьютерной грамотности, поскольку только тогда возникает понимание того, как современные технические средства могут превратиться в инструмент получения новых знаний.

Коренные преобразования в нашей стране, 90-х гг. XX в., повлекшие смену политических и экономических основ Российского государства, связаны с существенными изменениями идеологии, социальной структуры общества и реформированием правовой системы. Возникла потребность в осознании каждым человеком своего нового социального статуса, положения в социально неоднородном обществе. Процесс становления новых законов и правовых норм идет постепенно, что усиливает правовую напряженность в обществе. Познание законов, становление правосознания населения может способствовать установлению стабильности социальных отношений в стране.

В этих условиях социально-правовая компетентность может стать для молодого поколения важной основой в его гражданском самоопределении.

Успех общества, в котором каждый человек может реализовывать свои права и свободы, во многом зависит от нравственной и правовой воспитанности граждан. Однако разработка педагогических основ социально-правовой компетенции учащегося не получила глубокого решения в школьной программе. Хотя в научных трудах педагогов и правоведов указывается, что в стремлении к свободе и независимости реализуется сущность основных ценностей человека, его созидательной предназначенности и направленности личности на выполнение социально-правовых действий, дисциплинирующих человека и укрепляющих порядок в обществе. К сожалению, у многих будущих учащихся нет для этого необходимых знаний, а те, которые имеются, не всегда личностно значимы. Большинство учащихся, вступая в социально-правовые отношения, часто не умеют проявить себя в реальной жизни, не могут воспользоваться представленными им правами и свободами, порой не видят их органической связи со своими обязанностями. Недостаток в правовом воспитании учащихся, особенно в нравственной аргументации правовых явлений и, наоборот, невнимание к негативным явлениям общественной жизни, противоправному поведению граждан, приводит к деформации социально-правовых отношений.

Профессор Зеер Э.Ф. определяет социально-правовую компетенцию как знания и умения в области взаимодействия с общественными институтами и людьми, а также владение приемами профессионального общения и поведения. При этом профессор Зеер Э.Ф. выделяет следующие правовые ЗУНы: знание системы российского законодательства, а в частности нормативной базы по полученной специальности, знания структуры нормы права, умение применять нормы права в профессиональной деятельности, решать правовые ситуации на рабочем месте, пользоваться правовой базой в электронном варианте.

Социально-правовую компетенцию можно определить следующим образом: социально-правовая компетентность – это знание государственных правовых актов, документов, в области профессиональной деятельности, навыки общения при работе с людьми и документами, критический подход к своей деятельности, работа с нормативно-правовой документацией.

Социально-правовая компетенция, являясь частью информационной компетентности (А.А. Кузнецов, М.П. Лапчик), представляет собой знания и умения в области взаимодействия с общественными институтами и людьми, а также владение приемами коммуникации в

социуме правовыми способами. Можно выделить следующие компоненты социально-правовой компетенции:

- знания об авторских правах и мерах по их защите, этических и правовых нормах информационной деятельности человека, информационной безопасности и информационной культуре;
- умения использования информационных ресурсов общества с соблюдением соответствующих правовых и этических норм, программные средства создания информационных объектов, организации личного информационного пространства, защиты информации;
- навыки поиска, сбора, хранения информации и использования разнообразных методов для обеспечения защиты информации;
- использовать приобретенные знания и умения в практической деятельности и повседневной жизни для передачи информации по телекоммуникационным каналам в учебной и личной переписке, использования информационных ресурсов общества с соблюдением соответствующих правовых и этических норм, использование правил ограничения доступа для обеспечения защиты от компьютерных вирусов.

Говоря о социально-правовой компетенции, можно выделить следующие виды деятельности этого направления, характерные для уроков информатики:

- владение формами устной речи (монолог, диалог, полилог, умение задать вопрос, привести довод при устном ответе, дискуссии, защите проекта и т.п.).
- ведение диалога «человек» - «техническая система» (понимание принципов построения интерфейса, работа с диалоговыми окнами, настройка параметров среды и т.д.).
- умение представить себя устно и письменно, владение стилевыми приемами оформления текста (электронная переписка, сетевой этикет, создание текстовых документов по шаблону, правила подачи информации в презентации и т.п.).
- владение телекоммуникациями для организации общения с удаленными собеседниками (понимание возможностей разных видов коммуникаций, нюансов их использования и т.д.).
- понимание факта многообразия языков, владение языковой, лингвистической компетенцией (в том числе - формальных языков, систем кодирования, языков программирования; владение ими на соответствующем уровне).
- умение работать в группе, искать и находить компромиссы (работа над совместным программным проектом, взаимодействие в Сети, технология клиент-сервер, совместная работа приложений и т.д.).
- толерантность, умение строить общение с представителями других взглядов (существование в сетевом сообществе, телекоммуникации с удаленными собеседниками и т.п.) [1].

Формирование у учащихся социально-правовой компетенции на уроках информатики, это овладение ими комплексом универсальных правовых действий, структура которых предполагает взаимосвязь личностных и социально-ценностных качеств, определяющих его готовность и способность к естественной адаптации в социуме при решении проблем жизнедеятельности на основе саморазвития, самореализации, взаимопонимания и взаимодействия с другими членами общества правовыми способами.

***Библиографический* список**

1. Зимняя И.А. Ключевые компетентности как результативно-целевая основа компетентностного подхода в образовании. Авторская версия. - М.: Исследовательский центр проблем качества подготовки специалистов, 2004.
2. Лапчик М.П. Методика преподавания информатики: учеб. пособие для студ. пед. вузов. - М.: издательский центр «Академия», 2007. – 624 с.
3. Равен Дж. Компетентность в современном обществе. - М., 2002.
4. Чкалова Н.В. Формирование коммуникативной компетентности учащихся средствами информатики [Электронный ресурс] Фестиваль педагогических идей «Открытый урок». - Режим доступа: http://festival.1september.ru/articles/415466/, свободный.

Старков А.Н.
к. п. н., доц. каф. информационных технологий
Крюкова В.Д., Мусыгина А.А.
студентки ф-та информатики

ОСНОВНЫЕ ВИДЫ И ФОРМЫ ПРОЯВЛЕНИЯ КИБЕРЭКСТРЕМИЗМА В МОЛОДЕЖНОЙ СРЕДЕ

ФГБОУ ВПО «Магнитогорский государственный университет»,
Anyutka_musik@mail.ru, redji90@mail.ru

Аннотация

В статье описаны основные виды киберэкстремизма. Рассмотрены проявления видов киберэкстремизма. Представлены рекомендации по выявлению киберэкстремизма.

В настоящее время сложно представить жизнь общества без информационно-коммуникационных технологий, которые играют решающую роль в промышленном производстве, определяют экономическую и политическую динамику. Интернет стал неотъемлемой частью жизни людей. В связи с глобальной компьютеризацией общества, появилась такая проблема как киберэкстремизм.

Киберэкстремизм – это экстремизм в сети Internet. Экстремизм проще всего определить как склонность и приверженность личности или группы лиц к крайним взглядам или действиям. Чаще всего этим словом обозначают радикальные общественные движения – террористическая деятельность, возбуждение социальной, расовой, национальной или религиозной розни и т.д.

Во всех видах экстремизма присутствуют общие черты: угроза, фанатизм, одержимость в стремлении навязать свои принципы и взгляды оппонентам; опора на чувства, инстинкты, предрассудки, а не на разум; неспособность к толерантности, компромиссам либо игнорирование их.

Молодежь, особенно в возрасте 13-22 лет является более подверженной экстремистским идеям, т.к. является активным и основным пользователем Интернета. Этому возрасту присуще обостренное чувство справедливости, попытка самовыражения, поиск ценностей и смысла жизни. Кроме того, в это время подросток озабочен желанием найти свою группу, поиском собственной идентичности, которая формируется по самой примитивной схеме «мы» - «они». Также этому возрасту присуща неустойчивая психика, легко подверженная внушению и манипулированию. Этим подсознательным запросам как нельзя лучше соответствуют экстремистские субкультуры с их четким разделением на «наших» и «не наших» и четко провозглашенными границами добра и зла (а также зримыми образами этого зла в лице «чужих» - негров, евреев, кавказцев и т.д.).

В результате в последние годы происходит обострение проблемы молодежного экстремизма, который в настоящее время может рассматриваться как проблема общегосударственного значения и угроза национальной безопасности России.

Киберэкстремистская деятельность молодежных неформальных объединений осуществляется в отношении властных структур, отдельных политиков, объединений, социального строя или социальных групп, религиозных общин, религиозных деятелей, наций, народностей и т.д.

Исследование форм проявления киберэкстремизма в молодежной среде имеет важное значение для деятельности государственных правоохранительных органов и спецслужб по предупреждению правонарушений со стороны молодежных неформальных объединений в современных условиях. Внедрение экстремизма в молодежную среду в настоящее время приобрело очень большие масштабы и имеет опасные последствия для будущего нашей страны, так как подрастающее поколение – это ресурс национальной безопасности, гарант поступательного развития общества и социальных инноваций.

Молодежные неформальные объединения в сети представляют собой стихийно формирующиеся общности, которые сами создают структуру. В них действуют не установленные извне нормы, которые не фиксируются в уставах и инструкциях, а стихийно возникают в процессе общения, в результате чего воспринимаются всеми их членами и укореняются, превращаясь в индивидуальные специфические установки и ценностные ориентации. Неформалы имеют различный уровень организованности. В одних объединениях отсутствует четкая структура по какому-либо признаку, в других есть стабильный состав, лидер, руководящее ядро, существует распределение ролей.

На одном из слушаний в Государственной думе заместитель генерального прокурора РФ Виктор Гринь заявил, что «Интернет – это рассадник экстремизма». В связи с этим генпрокуратура предложила законодательно упорядочить деятельность Интернета. Такие предложения возникли не впервые, но до сих пор подобные попытки были тщетны. Виктор Гринь возмущен тем, что в интернете можно прочитать о том, как сделать бомбу и взорвать жилой дом. Он также указал на то, что реальные преступники пользовались взятыми из Интернета сведениями для совершения преступлений, о чем говорят данные из многих уголовных дел в России.

Наиболее ярко проявились такие формы экстремизма как экономически, политический, националистический, религиозный, экологический, духовный, которые находят проявление в виде молодежного киберэкстремизма.

1. Экономический экстремизм направлен на ликвидацию многообразия и установление какой-либо одной формы собственности, единых методов ведения хозяйства, полный отказ от принципов государственного регулирования экономической сферы[6]. Источником политического экстремизма является деятельность лиц, создающих предпосылки для разрушения экономики, Вооруженных Сил, систем образования и здравоохранения [6].

Ниже представлен случай политического экстремизма:

Год назад писатель и блогер Олег Шинкаренко разместил в своем Живом Журнале фотографию с изображением Виктора Януковича и риторический вопрос внизу о том, кто и когда наконец убьет президента. 30 июля к нему подошли трое, представились работниками СБУ и пригласили «на беседу».

Просто так беседовать Шинкаренко не захотел, но на следующий день ему вручили официальную повестку. Пообщавшись со следователями, блогер написал объяснительную, в которой называл свои действия «проявлением эмоций». Вскоре запись с ЖЖ Шинкаренко исчез. Сам писатель уверял тогда, что его не удалял, по его мнению, это могли сделать те же стражи.

И история стала первой громкой попыткой украинских спецслужб противодействовать политическому онлайн-экстремизма, как они его себе представляют. Поэтому она вызвала громкий скандал: за Шинкаренко в конце концов даже «вступился» сам Янукович, заявивший, что «не поддерживает» в этом деле действий СБУ [7].

2. Религиозный экстремизм проявляется в нетерпимости к представителям других конфессий или жестком противоборстве в рамках одной конфессии [6].

Приведем случай проявления религиозного киберэкстремизма:

Недавно мировой судья участка № 16 вынес решение в отношении мужчины, который в онлайновом обсуждении возможного возведения мечети допустил высказывание, призывающее к расправе над лицами определённого вероисповедания.

Несмотря на то, что комментарий был удалён в короткий промежуток времени, его успели заметить.

Были проведены лингвистическая и психолого-социальная экспертизы, которые установили, что высказывание содержит призыв, направленный на возбуждение религиозной вражды, а также призыв к совершению преступлений по мотивам религиозной вражды или ненависти.

Российское и международное право гарантирует свободу мысли и слова. Однако общемировое право запрещает возбуждение социальной, расовой, национальной или религиозной ненависти и вражды, социального, расового, национального, религиозного или языкового превосходства.

Суд вынес решение: виновен в преступлении, предусмотренном ч.1 ст.280 УК РФ. Назначенное наказание — штрафа в размере 40 тысяч рублей [8].

3. Экологические экстремисты выступают против не только эффективной природоохранительной политики, но и научно-технического прогресса вообще [6].

4. Духовный экстремизм ориентирован на изоляционизм, отвергает опыт, достижения другой культуры, навязывает в качестве официальной идеологии определенные социальные, религиозные, этнические стандарты [6].

5. Националистический экстремизм отвергает интересы, права других наций, провозглашает верховенство одной нации над другими [6].

Приведем случаи проявления националистического киберэкстремизма:

Студент задержан за экстремистские призывы в социальной сети.

Задержанный по просьбе своего приятеля по Интернет-сообществу, проживающего в другом регионе, разместил на собственной странице в социальной сети экстремистское обращение.

«Суть обращения состояла в приглашении молодых людей определенных национальностей собраться вместе и решить, как противостоять угрозе, исходящей, по их мнению, от граждан нашей страны другой национальности. Тем, кто решил отсидеться и остаться в стороне от событий, адресовались гневные строки, написанные с тонким расчетом на национальный колорит и традиции», - отмечается в сообщении УВД.

Студент адаптировал присланный ему из другого региона текст к местным реалиям и назначил место встречи и время [1].

Стоит задумываться, прежде чем размешать у себя в социальной сети какие-либо обращения и встречи, не является ли это противозаконным. Если вас попросили разместить у себя в социальной сети какую-либо информации, перед этим ее нужно внимательно прочитать. И если она содержит признаки экстремизма, например: оскорбление других наций, другую веру, цвет кожи и т.д., то размещать такого рода информацию, запрещено. А если вы сознательно размещаете такую информацию, то не надейтесь, что за это ничего не будет.

Студента оштрафовали за пропаганду экстремизма.

Юноше придется раскошелиться на 20 тысяч рублей. Такой приговор 25 октября 2011 года вынес Советский райсуд Челябинска.

По материалам дела, обвиняемый в 2009-2010 годах создал в соцсети тематическую группу пользователей, в которой размещал экстремистские материалы. Участники группы пропагандировали расизм и насилие по отношению к иностранцам. За год в виртуальную компанию влилось более 600 человек, в том числе жители Украины и других государств [2].

Распространение Расизма и нацизма в России, даже в сети Интернет является противозаконным. Если вы обнаружили группу или форум такого рода, то следует информировать администраторов сайта. А если вы узнали о существовании такого сайта, то следует обратиться в правоохранительные органы, что бы он приняли необходимые меры.

Студента могут посадить за экстремизм в Интернете.

19-летний камчатский студент обвиняется в совершении преступления, предусмотренного ч. 1 ст. 282 УК РФ (возбуждение ненависти либо вражды, а равно унижение человеческого достоинства), за размещение в интернете видеоматериалов, запечатлевших убийство гастарбайтеров. Парню грозит до четырех лет лишения свободы [5].

Разжигание ненависти к людям другой расы из-за ролика в Интернете.

Как сообщают СМИ, 20-летнему студенту ТГУ грозит двухлетнее лишение свободы за размещение экстремистского видеоролика в социальной сети «Вконтакте». В отношении парня было возбуждено уголовное дело о ненависти либо вражде по признакам пола, религии, принадлежности, языка, расы и национальности. Об этом сегодня заявили в следственном комитете Томской области.

Следствием был обнаружен видеоролик, который строился на международной розни, в разделе «видеозаписей» в соцсети Вконтакте. Оперативно выяснив личность интернет-пользователя, разместившего ролик, следователями СК РФ был проведен обыск по месту его проживания. После чего был задержан молодой человек, которые на допросе признался в содеянном. В данный момент студент находится под подпиской о невыезде. Ему грозит наказание в виде штрафа или лишения свободы до двух лет. По словам самого владельца соцсети Павла Дурова, данный случай показывает способность правоохранительных органов следить за порядком в виртуальном мире [3].

В России мало внимания уделяют просвещению общества, о том что можно размещать в сети, а что нельзя. В данных случаях, люди возможно не подозревали о том, что видео такого характера размещать в сети нельзя. Из чего следует, что нужно поднимать уровень просвещенности общества о законах связанных с сетью Интернет.

В Саратове за экстремизм задержан бывший правоохранитель – ругал русских на форуме.

Саратовские стражи порядка развеяли миф об анонимности в Сети: 50-летний мужчина стал фигурантом дела об экстремизме, поучаствовав в дискуссии на сайте ИА "Взгляд-инфо". Подозреваемый написал уничижительный комментарий о русских и евреях, а при задержании не стал отрицать своей вины.

Главный редактор агентства Николай Лыков, увидев оскорбительный комментарий, заявил на анонимного интернет-пользователя в полицию и в Следственный комитет. Нарушителя этики и спокойствия нашли сравнительно быстро: свой отзыв мужчина оставил 24 сентября, 19 октября материалы проверки, проведенной органами, была доставлена в СКР по Саратовской области, а 25 октября было заведено уголовное дело по ч. 1 ст. 282 УК РФ (экстремизм).

Подозреваемым стал мужчина 50 лет, который в прошлом работал в правоохранительных органах. Он дал признательные показания, и следователи отпустили его под подписку о невыезде. В ходе обыска у мужчины был изъят системный блок компьютера.

За какое именно высказывание завели дело на интернет-пользователя, неизвестно - его комментарий был удален из обсуждения на сайте по обращению Роскомнадзора.

Отметим, что для того чтобы оставить отзыв под новостью, на сайте не требуется никакой регистрации: достаточно ввести какой-то текст в поле "Ваше имя". Поэтому в обсуждении под новостью, например, про местного атамана Илью Майорова появляются несколько комментариев под заголовками: «Майоров», «Тоже майоров», «Еще Майоров». Что касается 50-летнего бывшего стража порядка, то он свой комментарий озаглавил «Все вы клоуны» [4].

Этого следовало ожидать! Создавая данный форум, в котором интернет-пользователи могут анонимно высказывать свое мнение. Полный простор для «грязи». Люди так устроены, им нужны скандалы, споры и т.п. Но анонимность на форуме не дает право оскорблять других людей и высказывать экстремистские высказывания, ведь за это придется понести наказание.

Омский студент-экстремист получил 100 часов обязательных работ

В сентябре 2010 года четверокурсник Омского промышленно-экономического колледжа Андрей Черноусов с домашнего компьютера выходил в интернет и размещал там "рисунки, фотографии и тексты, пропагандирующие нацистскую атрибутику и символику". Вдобавок омич изготовил баннер с аналогичным содержанием и повесил его на остановке транспорта "Телецентр". На этом деятельность поклонника Гитлера не остановилась – Черноусов рисовал нацистские лозунги и символику на стенах жилых домой и постройках города. Экстремистские действия в итоге пресекли сотрудники регионального Управления ФСБ России, установившие личность приверженца нацистской идеологии. Кировский районный суд г. Омска признал студента виновным по ч. 1 ст. 282 УК РФ Приговором от 22 октября Черноусову назначено наказание в виде 100 часов обязательных работ [9].

«Поклонник» Гитлера пропагандирующий нацистскую атрибутику и символику, думал что ему все сойдет с рук, но в конце концов, он понес за это наказание. Поэтому прежде чем совершать экстремистские деяния как в сети так и в реальности, стоит задуматься о последующей ответственности за свои действия.

Интернет наводнен всевозможными экстремистскими высказываниями, музыкой, видео, картинками, сообществами и т.д. что является рассадником киберэкстремизма, поэтому необходимо ужесточить контроль модераторами форумов и администраторов социальных сетей за подобной информацией, пресекать и своевременно сообщать правоохранительным органам об обнаружении киберэкстремистских явлений.

Публикация выполнена при поддержке гранта РГНФ № 13-06-00156 «Подготовка педагогических кадров к профилактике и противодействию идеологии киберэкстремизма среди молодежи»

Библиографический список

1. Тюменский студент задержан за экстремистские призывы в соцсети[статья] Деловая газета:Взгляд - [Электронный ресурс]. URL: http://vz.ru/news/2010/12/14/454775.html (дата обращения: 05.05.2013)

2. Челябинского студента оштрафовали за пропаганду экстремизма в соцсети. - УралИнформБюро - [Электронный ресурс]. URL: http://www.uralinform.ru/news/crime/142136-chelyabinskogo-studenta-oshtraphovali-za-propagandu-ekstremizma-v-socseti/ (дата обращения: 05.05.2013)

3. Студента из Томска могут посадить в тюрьму за видеоролик в соцсети «Вконтакте». - Лига Новости. - [Электронный ресурс]. URL: http://newsliga.ru/index.php?nma=news&fla=stat&nums=27565 (дата обращения: 05.05.2013)

4. В Саратове за экстремизм задержан бывший правоохранитель - ругал русских на форуме. - NEWSru.com. - [Электронный ресурс]. URL:http://www.newsru.com/russia/26oct2012/saratov.html(дата обращения: 05.05.2013)

5. Студента могут посадить за экстремизм в интернете. - Русский обозреватель. - [Электронный ресурс]. URL: http://www.rus-obr.ru/days/8661 (дата обращения: 05.05.2013)

6. Экстремизм. Виды экстремизма. Уголовная ответственность. - [Электронный ресурс]. URL: http://school7-66.3dn.ru/forum/15-161-1 (дата обращения: 05.05.2013)

7. Тролль-контроль. –Informer.cn.ua.-[Электронный ресурс]. URL: http://informer.cn.ua/novosti_chernigova/troll-kontrol/ (дата обращения: 05.05.2013)

8. Житель Кирово-Чепецка осуждён за комментарий на сайте . – Kirovcity.ru -[Электронный ресурс].
URL:http://www.kirovcity.ru/news/kirov/20326 (дата обращения: 05.05.2013)

9. Омский нацист рисовал свастики на стенах домов. – Омскпресс-[Электронный ресурс].URL:http://omskpress.ru/news/35137/omskiy_natsist_risoval_svastiki_na_stenax_domov/ (дата обращения: 05.05.2013)

Старков А.Н,
к. п. н., доц. каф. информационных технологий,
Сафрина С.В., студентка факультета информатики

СПЕЦИФИКА ПРОФИЛАКТИКИ ПРОЯВЛЕНИЙ КИБЕРЭКСТРЕМИЗМА В МОЛОДЁЖНОЙ СРЕДЕ

ФГБОУ ВПО «Магнитогорский государственный университет»,
sveta.brosslovski@mail.ru

Аннотация

В статье описаны основные понятия экстремизма и киберэкстремизма. Описано влияние виртуальной среды на развитие экстремистских наклонностей у населения. Так же представлены примеры экстремизма зарубежных стран. Прописана специфика проведения профилактических действий, направленных на уменьшение числа экстремистско-настроенных людей.

Молодёжь – самая подверженная киберэктремизму группа населения. Это обусловлено рядом факторов. Во-первых, молодые люди и девушки большую часть своего времени проводят в виртуальном мире, а именно: общаются в социальных сетях, «сидят» день и ночь в чатах, смотрят фильмы, видеоролики, качают софт для своего ноутбука или планшета, играют в он-лайн игры и многое другое. Еще одним немаловажным фактором является юношеский максимализм. В 15-20 лет молодёжь особенно трепетно относится к проблемам, воспринимает информацию больше эмоционально, нежели рационально. Поэтому чаще всего киберэктремизму подвержены молодые «горячие» головы, желающие изменить всё, всех, и сиюминутно. В- третьих, любопытство молодым людям не занимать. Всё новое и неизведанное вызывает у них дикое желание попробовать, посмотреть, поучаствовать. Поэтому любое новое течение, навеянное модой, принимается нашей молодёжью на ура, ведь это такая прекрасная возможность выделиться, не быть как все, выразить свою точку зрения, проявить внутренние таланты, вступая в то или иное течение.

Обратимся к понятию экстремизма. Экстремизм – это идеология допустимости использования крайних мер, экстремумов социального поведения, для получения желаемого эффекта [8]. Он может быть политическим, религиозным, экономическим, социальным и т.п., вплоть до бытового. Это определение описывает саму суть и подчёркивает, что экстремизм использует крайние меры, и не стремится к компромиссу.

Согласно ст. 1 ФЗ «О противодействии экстремистской деятельности» от 25 июля 2002 г. N 114-ФЗ под экстремисткой деятельностью (экстремизмом) понимаются:

1) насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации;

2) публичное оправдание терроризма и иная террористическая деятельность;

3) возбуждение социальной, расовой, национальной или религиозной розни;

4) пропаганда исключительности, превосходства либо неполноценности человека по признаку его социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии;

5) нарушение прав, свобод и законных интересов человека и гражданина в зависимости от его социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии.

6) совершение преступлений по мотивам, указанным в п. «е» ч.1 ст. 63 УК РФ (совершенные по мотивам политической, идеологической, расовой, национальной или религиозной ненависти или вражды в отношении какой-либо социальной группы)

7) пропаганда и публичное демонстрирование нацистской атрибутики или символики либо атрибутики или символики, сходных с нацистской атрибутикой или символикой до степени смешения;

8) публичные призывы к осуществлению указанных деяний либо массовое распространение заведомо экстремистских материалов, а равно их изготовление или хранение в целях массового распространения [9].

Отметим, что в российском законодательстве не определены понятия политического и религиозного экстремизма, среди специалистов продолжается дискуссия о правомерности использования данных терминов и их содержании.

Рассмотрим юридические определения экстремизма в США. Подобные преступления в некоторых штатах США квалифицируются как «преступления на почве ненависти». Это специальная юридическая квалификация особого рода преступлений против личности, совершаемых под влиянием ненависти к лицам иной расы или национальности, вероисповедания, этнического происхождения, политических убеждений, пола и сексуальной ориентации, инвалидам. Такая дополнительная квалификация, отягчающая вину и ужесточающая наказание, существует в некоторых штатах США, в ряде стран Западной и Центральной Европы, но отсутствует в других штатах и государствах [8].

Примером применения данного закона может выступить история о FtM транссексуале Тине Рене Брэндоне, получившим известность как жертва преступления на почве ненависти. Его убийство привлекло широкое общественное внимание к проблеме

насилия над представителями сексуальных меньшинств и способствовало активизации борьбы за расширение законодательного определения «преступления на почве ненависти» на понятия «сексуальная ориентация» и «гендерная идентичность». Судьба Брэндона Тины послужила сюжетной основой для ряда художественных произведений.

Проводя данное исследование, мы провели опрос населения посредством анкетирования. В анкете был представлен один вопрос «Как вы относитесь к экстремизму?». С помощью результатов анкетирования мы хотели прояснить отношение обычных граждан к экстремизму. Горожане, принявшие участие в анкетировании, относятся к разным возрастным и социальным группам, профессиям.

Алексей, менеджер, 30 лет: «Экстремизм – это реальная угроза, остальные глобальные проблемы – просто пыль в сравнении с ним. Знаю, что молодежь вовсю вербуют через социальные сети. По крайней мере, к наркомании таким образом приобщают точно. Завлекают их очень просто: некие милые девочки пишут парням, все внешне невинно. Но вот, допустим, у парня депрессия. А новая знакомая очень кстати предлагает встретиться или приходит домой. И у нее уже готова доза. Угощайся, причем, бесплатно – это должно утешить. У экстремистов подобные средства тоже в ходу. Всем известно, призывы выступить на Манежной распространялись именно через социальные сети».

Светлана, 20 лет, студентка: «Что такое экстремизм? Это настоящий современный нацизм. Когда те, кому нечего делать, объединяются, чтобы «чистить» город от приезжих. Я против этого».

Екатерина, медсестра, 37 лет: «Экстремизм – это боевики, терроризм, женщины в черной одежде… Это те, кто против власти, те, кто ее ненавидит и всячески это демонстрирует…»

Надежда, директор сети магазинов, 50 лет: «Экстремистам кажется, что они борются за свои права. Пусть даже этот способ не одобряет мировое сообщество, им плевать. Они же экстремисты и идут напролом. Конечно, я против такого явления в нашей жизни».

Делая вывод из вышесказанного, отметим, что большая часть опрошенных относится негативно к этому явлению и не одобряет проявление экстремизма среди масс.

Экстремизм может предстать перед нами абсолютно в любом проявлении.

К примеру, в России весьма распространена гомофобия. По сравнению с Западной культурой, уровень ненависти и нетерпимости к представителям сексуальных меньшинств гораздо выше. В экспресс-опросе ВЦИОМ в феврале 2001 г. был предложен такой вопрос: «Люди очень по-разному относятся к гомосексуалистам и лесбиянкам.

Как Вы лично думаете, это - …». Вариант «распущенность, вредная привычка» выбрали 36% опрошенных, «болезнь или результат психической травмы» - 31%, «сексуальная ориентация, имеющая равное с обычной право на существование» - 20%, «признак особой одаренности, таланта» - 1%, «затрудняюсь ответить» – 12%. В марте 2002 г. при опросе москвичей от 20 до 45 лет, на вопрос «Как Вы считаете, это нормально, допустимо – иметь половые контакты с партнером своего пола?» утвердительно ответили около 12%, отрицательно – 76%, 12% затруднились ответом.

Экстремизм на почве гомофобии перетек и в глобальную паутину. Интернет пестрит призывами искоренять гомосексуализм из масс. А также лозунгами, с ненормативной лексикой, оскорбляющей людей другой ориентации. Также в соцсетях ежедневно создаются группы с экстремистским содержанием по отношению к представителям гей-сообщества.

Еще одним проявлением экстремизма, которое мы рассмотрим в нашей статье, пропаганда нетерпимости на религиозной почве.

Религиозный экстремизм следует рассматривать как крайнюю форму религиозного фанатизма. Суть любого экстремизма, в том числе и религиозного, – в применении насилия к инакомыслящим. Религиозный экстремизм – это как раз приверженность к крайним взглядам и мерам в стремлении переустройства мира в соответствии с религиозной фанатической идеологией. Основная цель религиозного экстремизма – признание своей религии ведущей и подавление других религиозных конфессий через их принуждение к своей системе религиозной веры. Наиболее ярые экстремисты ставят своей задачей создание отдельного государства, правовые нормы которого будут заменены нормами общей для всего населения религии. Религиозный экстремизм часто смыкается с религиозным фундаментализмом, суть которого заключена в стремлении воссоздать фундаментальные основы «своей» цивилизации, очистив ее от чуждых новаций и заимствований, вернуть ей «истинный облик». Противодействие экстремизму осуществляется по следующим основным направлениям: принятие профилактических мер, направленных на предупреждение экстремизма, в том числе на выявление и последующее устранение причин и условий, способствующих его осуществлению; выявление и пресечение экстремизма; международное сотрудничество в области противодействия экстремизму.

В целях противодействию и профилактике распространений идей религиозного экстремизма, терроризма и сепаратизма Департаментом юстиции совместно с Департаментом внутренней политики, Православной церкви и правоохранительными органами проводится ряд профилактических мероприятий.

Мощным средством противодействия распространению экстремизма может стать активная пропаганда духовно-нравственных ценностей и традиций наших народов: их патриотизма, веротерпимости, присущего им обостренного чувства ответственности за судьбу будущих поколений, векового опыта преодоления жизненных трудностей совместными усилиями [10].

В качестве примера религиозного экстремизма можно привести монологи Эрика Картмана, мультипликационного героя, сериала Южный парк. В них он выражает свою ненависть к Иудаизму и еврейской нации. Так же Эрик пропагандирует национальный, расовый экстремизм. На протяжении сериала, герой не раз высказывал мысль о том, что ему близка политическая позиция Адольфа Гитлера. А так как сериал доступен просмотру широкой аудитории, то можно сделать вывод о том, что идеи расового экстремизма могут повлиять на мировоззрение подрастающего поколения. Велика вероятность, что молодежь может воспринять монологи Эрика не как шутки и юмор, а как реальные идеи расизма, нетерпимости и насилия.

С развитием интернет пространства, экстремизм перенесся и виртуальную среду. В связи с этим, ученые присвоили ему название – киберэкстремизм. Это могут быть, например, статьи в блогах. Группы и странички в соцсетях пестрят заголовками: «Я – русский!», «Фашизм, антифа, скинхеды, расизм», «Мы сохраним белый мир». Эти названия, взятые нами из соцсети «Вконтакте», далеко не единственные. Помимо этого существуют отдельные сайты, посвященные пропаганде экстремизма, на которых размещены лозунги, призывы, провокации. Такое изобилие экстремистской информации, по нашему мнению, пагубно сказывается на мировоззрении юных людей. Приведём немного статистики. На учете в органах внутренних дел состоит свыше 450 молодежных группировок экстремистской направленности общей численностью около 20 тысяч человек. Членами экстремистских группировок становятся, как правило, молодые люди 16-25 лет. В 2009 году было зарегистрировано 548 преступлений экстремистской направленности, что на 19% больше, чем в 2008 году, при этом раскрыты только 484. По данным МВД России на 2007 год, в стране около 98 тыс. подростков являлись членами группировок антиобщественного, экстремистского и иного характера. Статьи экстремистского характера, распространённые в виртуальной сети, пагубно влияют на психику молодых людей, считает Пономарёв Михаил Сергеевич кандидат психологических наук, педагог-психолог [6].

Одним из самых ярких представителей киберэкстремизма и экстремизма в молодёжной среде в России, по праву является Марцинкевич Максим Сергеевич, известный больше, как «Тесак».

Этот молодой человек, будучи студентом третьего курса московского вуза, организовал нацистскую группировку. Являясь её непосредственным предводителем, Максим снимал видеоролики о людях нерусской национальности, в которых издевался и применял насилие по отношению к «главным героям». Этот материал был выложен во всемирную паутину. Как только ролики были опубликованы, о «Тесаке» узнало российское интернет сообщество. Огромное количество видеороликов с его участием находится в витруальной сети и до сих пор. В настоящее время Тесак несколько сменил профиль. Теперь он занимается проектом «Оккупай-педофиляй». Однако схема проекта аналогична: он с командой ловит и «троллит» своих «жертв». Но теперь дело уже касается потенциальных педофилов. Весь процесс также снимается на видео, и выкладывается в глобальной сети. У этого проекта появилось множество сторонников и последователей. Доказательством этому являются подобные сообщества, которые появляются в каждом городе России. Таким образом, можно сделать вывод, что Максим Марцинкевич является яркой фигурой в молодёжной эктремистской и киберэкстремистской среде, что может вызывать озабоченность старшего поколения [4].

Что касается профилактики киберэкстремизма, во-первых, по нашему мнению, она должна быть ненавязчивой. Ведь зачастую у подростков возникает желание действовать вопреки. Во-вторых, такой профилактикой должны заниматься родители, учителя, преподаватели, администрация города, государство. Родители должны рассказывать своим детям о толерантности, терпимости, доброте, понимании. Учителя и преподаватели, в свою очередь, могут устраивать открытые конференции, уроки, на тему киберэкстремизма, показывая пагубные последствия экстремистских действий. Администрация города может возложить на себя обязанность в проведении молодёжных праздников-акций «Против Экстремизма и Киберэкстремизма», с участием молодёжных групп, различных конкурсов. В свою очередь, государство должно уделить внимание соц. сетям, экстремистским сайтам и т.д. Работники специальных служб должны проводить мониторинг сегментов интернет пространства, выявляя подобные сайты, сообщества, группы, блоги, и прекращать их функционирование. В настоящий момент, этим занимается Роскомнадзор. Обратимся к информации в СМИ: «Реестр противозаконных сайтов заработал в Рунете 1 ноября. Туда будут вноситься, а затем блокироваться ресурсы, содержащие опасную информацию. Так законодатели решили защитить общество, в первую очередь детей, от порталов, распространяющих сведения о наркотиках, призывы к суициду и детскую порнографию. Сайты с таким контентом попадут в черный список и будут заблокированы в досудебном

порядке, если опасную информацию вовремя не удалят. В реестр также попадут интернет-ресурсы, которые суд признал нарушителями законодательства. Вести реестр поручено Роскомнадзору. МВД, Федеральная служба по контролю за оборотом наркотиков и Роспотребнадзор также уполномочены отправлять сайты в черный список» [7].

При выполнении этих правил, мы считаем, что количество людей, пропагандирующих экстремизм и киберэкстремизм существенно сократиться.

Профилактика каиберэкетремизма и экстремизма должна проводится постоянно, и не только среди молодёжи, но и среди старшего поколения. Ведь если экстремистские идеи заложены в головах родителей, то их дети, скорее всего, унаследуют эти взгляды, и в итоге, работа учителей, преподавателей, психологов окажется бессмысленной.

Работу по профилактике среди старшего поколения могут взять на себя организации предоставляющие рабочие места. Должны проводиться беседы с работниками, мероприятия на тему «Защитим детей от влияния экстремизма». С определённой периодичностью следует проводить встречи с психологом, который будет выявлять людей предрасположенных к экстремизму, и принимать какие либо меры по его искоренению, предварительно обговорив список этих мер с руководством данного работника.

В заключение хочется сказать, что экстремизм и киберэкстремизм это понятия, связанные с призывом получить результат насильственно, а так как насилие ещё никогда не приводило ни к чему хорошему, следовательно, и киберэкстремизм как и обычный экстремизм должен быть максимально искоренён в головах людей, в том числе и молодёжи, ведь за молодыми будущее, будущее без насилия, будущее толерантных, терпимых и добрых людей.

Публикация выполнена при поддержке гранта РГНФ № 13-06-00156 «Подготовка педагогических кадров к профилактике и противодействию идеологии киберэкстремизма среди молодежи».

Библиографический список

1. Форум о экстремизме. Автор: Истинавт [4.8K]-[Электронный ресурс], URL: http://www.bolshoyvopros.ru/questions/10421-chto-takoe-terrorizm-i-ekstremizm-kakaja-mezhdu-nimi-raznica.html (дата обращения: 05.04.2013)

2. Блог Самонкина Юрия Сергеевича-[Электронный ресурс], URL:http://samonkin.blog.ru/115381491.html (дата обращения: 10.05.2013)

3. Политология. Словарь. — М: РГУ. В.Н. Коновалов. 2010. Понятние «Экстримизм»-[Статья], URL:

http://dic.academic.ru/dic.nsf/politology/262 (дата обращения: 09.04.2013)
4. Максим Марцинкевич-[Статья], URL: http://lurkmore.to/Tecak (дата обращения: 14.04.2013)
5. Южный парк - [Статья], URL: Brian C. Anderson South Park Conservatives: The Revolt Against Liberal Media Bias. — Regnery Publishing, 2005. — 191 с. — ISBN 978-0-89526-019-2 (дата обращения: 07.05.2013)
6. Пономарев М. С. Психолого-педагогические технологии профилактики проявлений экстремизма в образовательной среде школы. URL: http://www.myshared.ru/slide/117411/ (дата обращения: 12.05.2013)
7. Опасные сайты Рунета начали заносить в чёрный список - [Статья], URL: Topadless.com (дата обращения: 30.04.2013)
8. Википедия «Экстримизм» - [Статья], URL:http://ru.wikipedia.org/wiki/%DD%EA%F1%F2%F0%E5%EC%E8%E7%EC (дата обращения: 11.05.2013)
9. ФЕДЕРАЛЬНЫЙ ЗАКОН от 25.07.2002 N 114-ФЗ (ред. от 25.12.2012 с изменениями, вступившими в силу с 06.01.2013) "О ПРОТИВОДЕЙСТВИИ ЭКСТРЕМИСТСКОЙ ДЕЯТЕЛЬНОСТИ" - [Статья], URL:http://www.referent.ru/1/95895 (дата обращения: 01.05.2013)
10. Религиозный экстремизм: сущность, причины, пути предотвращения - [Статья], URL:http://do.gendocs.ru/docs/index-249519.html (дата обращения: 03.05.2013)

Чернова Е.В.,
к.п.н., доц. каф. информационных технологий

СОЦИАЛЬНЫЕ СЕТИ И КИБЕРЭКСТРЕМИЗМ

ФГБОУ ВПО «Магнитогорский государственный университет», EChernova@masu-inform.ru

Аннотация

Статья акцентирует внимание на проблемах вовлечения молодежи в социальных сетях в экстремистскую деятельность и механизмах профилактики и противодействия киберэкстремизму .

В последние годы в России и странах СНГ отмечается активизация ряда экстремистских движений, ориентированных на вовлечение в свои ряды молодых людей. Именно молодежная среда является благодатной почвой для формирования радикальных взглядов, накопления негативного потенциала, готового к реализации по указанию «лидера». Экстремизм является одной из наиболее сложных социально-политических проблем современного российского общества, что связано, в первую очередь, с многообразием экстремистских проявлений, неоднородным составом организаций экстремистской направленности,

которые оказывают дестабилизирующее влияние на социально-политическую обстановку в стране [1].

Развернутое определение экстремизма (экстремистской деятельности) в национальном праве дано в ст.1 Федерального Закона «О противодействии экстремистской деятельности». Необходимо обратить внимание на те его элементы, реализация которых может быть осуществлена с использованием сети Интернет [2]. Во-первых, это размещение программных документов различных групп, содержащих информацию, побуждающую к насильственному изменению конституционного строя и нарушению целостности России, пропаганду исключительности, превосходства либо неполноценности граждан по признаку их отношения к религии, социальной, расовой, национальной, религиозной или языковой принадлежности и т.п. Интернет позволяет «легко, безопасно, дешево и без цензуры» распространять любую идеологию по всему миру (в том числе демонстрирование нацистской атрибутики или символики), что способствует формированию ранее не существовавшего единого неонацистского, расистского сообщества, которое вдохновляет своих членов на совершение актов насилия. Во-вторых, активно используются участниками террористических и экстремистских организаций информационные ресурсы Интернета, позволяющие быстро и без дополнительных затрат найти разнообразные данные о способах изготовления самодельных взрывных устройств, методах осуществления преступлений террористического характера. В-третьих, экстремистские группы используют Интернет для финансирования своей деятельности (финансирование сайтов через рекламу, трафики захождения на сайт и т.п.) либо иного содействия в планировании, организации, подготовке и совершении указанных действий (координация действий).

На сегодняшний день, сторонники экстремизма с легкостью могут использовать возможности, предлагаемые информационно-коммуникативными технологиями: создание и регистрация информационных ресурсов, направленных на формирование и поддержку определенного мнения по ключевым вопросам, на обмен опытом, на вербовку последователей и др., в различных социальных сетях созданы множество групп, целью которых является распространение информации экстремисткой направленности.

Попытки перевести экстремистские взгляды и движения в виртуальную реальность предпринимались давно. В 1995 г. бывший член Ку-Клукс-Клана Дон Блэк создал первый сайт экстремистского толка. В 1996 г. насчитывалось около 70 подобных сайтов. В марте 2006 г. их было уже свыше 6 тысяч. Говорит ли это об экспоненциальном росте числа приверженцев. Согласно данным научно-исследовательского института обороны Норвегии в прошедшем десятилетии многочислен-

ные террористические организации активно осваивали Интернет для вербовки новых сторонников и распространения пропагандистских материалов. Кроме того, виртуальное пространство неоднократно использовалось такими группировками, как «Аль-Каида» для устрашения предполагаемого противника. Определить реальное количество подобного контента сложно, так как чаще всего сторонний наблюдатель не осознает, что отдельная информация в Интернете имеет экстремистский подтекст. Для несведущих людей переговоры террористов выглядят как нечто обыденное. Часто в целях пропаганды экстремисты используют чаты или обычную рассылку.

Рассмотрим одну из популярных социальных сетей на предмет присутствия в ней экстремистских групп. Наиболее распространенные виды экстремизма:

- по национальному признаку;
- на религиозной основе;
- нетрадиционная сексуальная ориентация;
- субкультуры и различия во вкусах и пристрастиях.

Национальный экстремизм – явление, выражающееся в ненависти и негативном отношении к некоторым национальностям и людям, относящимся к этим национальностям. В данной социальной сети преобладают группы, связанные с антисемитизмом и неприятием лиц кавказской национальности. В подобных группах обсуждают методы «расправы» над лицами, которые причисляются к тем, кого возбраняет группа или сообщество. Создатели подобных групп стараются назвать свою группу и описать ее таким образом, чтобы человек, случайно открывший ее, не сразу понял, о чем здесь ведутся дискуссии. Однако есть и такие группы, которые открыто заявляют о своей ненависти к людям некоторой расы и свои намерения по отношению к ним. Такие группы активно призывают пользователей сети вступить в их ряды. Численность некоторых групп достигает нескольких тысяч человек. В обсуждениях групп каждая цитата, каждая фраза кипит ненавистью к определенной национальности и призывает вершить самосуд над носителями этой национальности. В обсуждениях групп каждая цитата, каждая фраза кипит ненавистью к определенной национальности и призывает вершить самосуд над носителями этой национальности.

Религиозный экстремизм – тенденция, выражающая отрицательную реакцию на приверженцев той или иной веры. В изучаемой нами социальной сети, экстремизм на религиозной основе проявляется в очень ожесточенной форме. Названия групп соответствующей тематики призывают к насилию и уничтожению некоторых религиозных конфессий, как традиционных, так и нетрадиционных. Чтобы сильнее передать негатив и эмоциональный настрой, создатели группы применяют ненормативную лексику для описания групп. Молодежь активно

обсуждает способы уничтожения ненавистной религии. К сожалению, в данных обсуждениях участвуют и люди довольно-таки солидного возраста, и вместо нравоучений и наставлении юных умов на путь истинный, еще больше подливают масла в огонь гневными высказываниями в поддержку намерений группы.

В экстремистских группах, посвященных неприятию нетрадиционной сексуальной ориентации, придумывают кровожадные способы их истребления. Некоторые пользователи не показывают своего лица, ставя на аватары всевозможные картинки, которые иногда могут быть непристойного или агрессивного содержания. Группы против сексуальных меньшинств многочисленны и не всегда тем, кто в них состоит, есть 18 лет. Подростки активно описывают ритуалы издевательства и наказания тех, кто, по их мнению, порочит человеческий род и недостоин жить. Лидеры подобных экстремистских групп активно выявляют своих сторонников в социальной сети, а иногда стараются «завербовать» тех, кто до встречи с подобной группой, относился к нетрадиционной сексуальной ориентации довольно-таки терпимо. Некоторые группы изначально делаются закрытыми, чтобы пробудить интерес к ним.

В рассматриваемой социальной сети огромное количество групп, призывающих уничтожать людей, выделяющихся из толпы, выглядящих как-то по-особенному, не так как все. Без особого труда можно найти группу, которая расскажет, а некоторые и покажут, как следует поступить с представителями различных субкультур или же с теми, кто предпочитает, к примеру, светлый цвет волос. Можно найти и группы, которые призывают разорить и уничтожить людей, играющих значимые социальные роли или просто тех, кто живет в достатке. Методы борьбы с теми, кто, по мнению создателей групп является людьми второго сорта, не отличаются от тех, что готовы применить в группах против каких-либо религий или национальностей. Однотипная злоба, ненормативная лексика и жестокость – вот то, что можно найти в группах против субкультур.

Анализ данной социальной сети показывает, что экстремизм в ней развивается с огромной скоростью, группы появляются каждый день и быстро набирают себе сторонников. Администрация сайта не успевает среагировать на появление антисоциальной группы, которая продолжает поливать грязью пользователей и разжигать вражду в обществе.

В целях профилактики и противодействия экстремизму, предотвращения конфликтов на национальной, религиозной, социальной и т.п. основе необходимо составить ряд мероприятий, направленных на:

- мониторинг социальных сетей на предмет экстремистских групп;

- организацию получения оперативной информации об экстремистских настроениях, о попытках дискредитации органов власти и их представителей, об активизации криминального элемента и участников различных экстремистских формирований из социальных сетей;
- патриотическое воспитание молодежи, нацеленное на неприятие ею идеологии насилия, религиозной, национальной нетерпимости и т.д.;
- просвещение молодого поколения в вопросе культурного, религиозного и др. многообразия жителей России, истории национальной нетерпимости, геноцида и других преступлений, вызванных экстремистской деятельностью;
- создание эффективной системы просвещения граждан об опасности терроризма, религиозной нетерпимости, геноцида и других преступлений, порожденных экстремизмом и национализмом;
- ознакомление молодежи с Федеральным законом N 114-ФЗ «О противодействии экстремистской деятельности», в котором определяются правовые и организационные основы противодействия экстремистской деятельности, устанавливается ответственность за ее осуществление;
- ознакомление молодежи с Федеральным списком экстремистских материалов.

Таким образом, одной из злободневных проблем современной России является популяризация молодежного экстремизма. Количество преступлений растёт, уровень насилия повышается, а характер экстремисткой деятельности становится всё более организованным. На данный момент времени информационные технологии являются эффективным средством формирования общественного климата по вопросам достижения политических, экономических и иных целей, а также влияния на различные слои граждан. Поэтому такие ресурсы как Интернет, а в частности, социальные сети, создают благотворную почву для объединения в неформальные группы. Разрешить проблему экстремизма в социальных сетях только запретительными мерами невозможно.

Экстремизм является социально-опасным явлением, губительно сказывающимся на климате в обществе. Через Интернет он распространяется с неимоверной скоростью, каждую минуту завоевывая все больше пользователей Всемирной паутины. Воспитывая будущее поколение, необходимо сделать акцент на гуманизме, толерантности по отношению к национальностям, вероисповеданию, обычаям, традициям, сексуальной ориентации, субкультурам и т.п.

Публикация выполнена при поддержке гранта РГНФ № 13-06-00156 «Подготовка педагогических кадров к профилактике и противодействию идеологии киберэкстремизма среди молодежи».

Библиографический список

1. Методические рекомендации по профилактике и противодействию экстремизму в молодежной // Наша молодежь. – 2011. – № 6. – С.40-41.
2. Номоконов В.А., Тропина Т.Л. Терроризм с помощью Интернета // Терроризм в России и проблемы системного реагирования. – М.: Российская криминологическая ассоциация, 2008. – 192 с.
3. Чусавитина Г.Н., Чернова Е.В. Толерантность как средство борьбы с экстремизмом и терроризмом // Современные проблемы науки и образования: тезисы докл. XLIII внутривуз. науч. конф. преп. МаГУ. – Магнитогорск. 2011. – С. 100 – 102.
4. Зеркина Е.В., Чусавитина Г.Н. Подготовка будущих учителей к превенции девиантного поведения школьников в сфере информационно-коммуникативных технологий. – Магнитогорск: МаГУ, 2008. – 184 с.

Чусавитин М.О.,
аспирант

МЕТОДИКА ПОСТРОЕНИЯ ИМИТАЦИОННОЙ МОДЕЛИ БИЗНЕС-ПРОЦЕССОВ В СИСТЕМЕ ARENA 12.0 ДЛЯ РЕШЕНИЯ ЗАДАЧ СОВЕРШЕНСТВОВАНИЯ СУНБ

НИУ ВШЭ, jelly.chews@gmail.com

На всех этапах жизненного цикла системы управления непрерывностью бизнеса (СУНБ) менеджеры должны постоянно отслеживать состояния бизнес-процессов и их составляющих, вырабатывать эффективные превентивные меры воздействия на потенциальные угрозы и определять способы реагирования на нештатные ситуации и сбои системы [1]. Очевидно, что эксперименты с реальными объектами, как правило, невозможны, а создание прототипов очень дорого. Одним из путей поиска решения данных проблем является применение компьютерного имитационного моделирования (ИМ). Проведение ИМ предполагает осуществление четырех основных этапов: построение модели одного или нескольких процессов, выполнение которых необходимо оптимизировать; запуск имитации выполнения процессов модели; анализ полученных показателей; повторение предыдущих этапов для альтернативных сценариев выполнения процесса и выбор наиболее оптимального.

Рассмотрим методику применения имитационного моделирования при исследовании воздействия деструктивных факторов на критичные бизнес-процессы компании. Закладывая в модель различные сценарии кризисных ситуаций, имевших место в прошлом, а также гипотетически возможных в будущем, будут получены оценки рисков экстремальных событий [2; 3 и др.].

Для построения имитационной модели выберем бизнес процесс «Составление коммерческого предложения», так как он обладает следующими критическими ограничениями: большая требовательность к быстродействию; непосредственная проекция на клиента; лицо компании в глазах клиента напрямую зависит от того, как быстро и бесперебойно выполняется этот процесс; большое число разнообразных подсистем, участвующих в функционировании процесса; разнообразие вероятных точек отказа.

Таблица 1

Основные переменные, влияющие на процесс составления коммерческого предложения

№	Наименование	минимальное	максимальное	вероятное
Входящие заявки				
1	Составление коммерческого предложения (КП) за день	288 шт. 16 в каждом из 18 офисов	400 шт. 20 в каждом, 20 офисов	360 в день
2	Консультация	10 в каждом, 20 офисов	17 в каждом, 20 офисов	270 в день
3	Расчет ежедневной отчетности	-	-	1 раз в день
4	Локальный расчет в финансовом калькуляторе	-	-	24 раза в день
Среднее время обработки				
5	Выяснение цели обращения клиента	1 мин	7 мин	3 мин
6	Интервьюирование клиента	5 мин.	30 мин	10 мин
Коммуникация и каналы связи				
7	Связь с сервером по каналу VPN	-	-	~10 сек.
8	Связь с сервером по каналу RDP	1 мин	10 мин	5 мин
9	Задержки передачи данных локальным провайдером связи	120 сек	420 сек	120 сек.
10	Передача данных основным провайдером ЦОД	1 сек	5 сек	3 сек
11	Передача данных резервным провайдером ЦОД	1 мин	3 мин	2 мин
Локальные вычисления				

№	Наименование	минимальное	максимальное	вероятное
12	Обработка подключения сервером шлюза RDP	0.5 мин	5 мин	2 мин.
13	Обработка подключения сервером VPN	0,5 мин	2 мин	1 мин.
14	Обработка задачи локальных вычислений	18 мин	90 мин	60 мин
15	Обработка терминальной сессии клиента	1 мин	10 мин	5 мин
16	Просмотр информации в системе	0,5 мин	5 мин	1 минут
17	Расчет коммерческого предложения	0,5 мин	10 мин	2 мин
18	Расчет дневных отчетов	5 мин	20 мин	30 мин
Статистические данные				
19	Соотношение режимов доступа	RDP 25%	VPN 75%	-
20	Распределение нагрузки между серверами приложений	1 сервер: 50%	2 сервер: 50%	Вручную
21	Распределение нагрузки между серверами ERP	1 сервер: авт. по сессиям	2 сервер: авт. по сессиям	3 сервер: авт. по сессиям

В процессе анализа построенной модели необходимо определить значимые переменные и основные параметры процесса, выявленные на этапе обследования предметной области (см. табл. 1).

По результатам отчетов и опроса сотрудников компании необходимо составить статистику сбоев и требуемого времени восстановления оборудования (см. табл. 2).

В рамках данной работы инструментарием для построения модели была выбран инструментарий имитационного моделирования Arena компании Rockwell Software [4]. Для удобства разделим модель создания коммерческого предложения на 5 подмоделей:

1. Обработка обращения клиента (Manage);
2. Региональный офис (Office Infrastructure);
3. Каналы связи в сети Интернет (Internet Communication);

4. Сервер приложений (App Server);
5. Система планирования ресурсов предприятия (ERP System).

Подмодель создается нажатием кнопки «Submodel» на панели инструментов Arena. Создаем 5 подмоделей, и называем их в соответствии с вышеуказанным перечнем.

Таблица 2

Статистика сбоев и требуемое время на восстановление основных ИТ сервисов компании

Источник	Время бесперебойной работы		Время на восстановление	
	Оборудование	ПО	Оборудование	ПО
Маршрутизатор CISCO ASA	>2 лет	4 мес	3-5 дней	5 мин
Инфраструктура офиса	3 мес	0	1-3 час	0
Сервер приложений	99.999%	2 мес	5 мин	10 мин
Сервер шлюза	99.999%	99 из 100	5 мин	5 мин
Axapta Operation Server	99.999%	4 дня	5 мин	15 мин
SQL сервер	99.999%	6 месяцев	5 мин	20 мин
Основной канал интернет	1 год	-	30мин	-
Региональный канал интернет	1 мес	-	1- час	-
Резервный канал связи	2 года	-	30мин	-

Двойным нажатием на подмодель выполняется переход на рабочую область этой модели. Далее перетаскиваем необходимые блоки на рабочее пространство. Структура имитационной модели обработки заявок клиентов представлена на рис. 1.

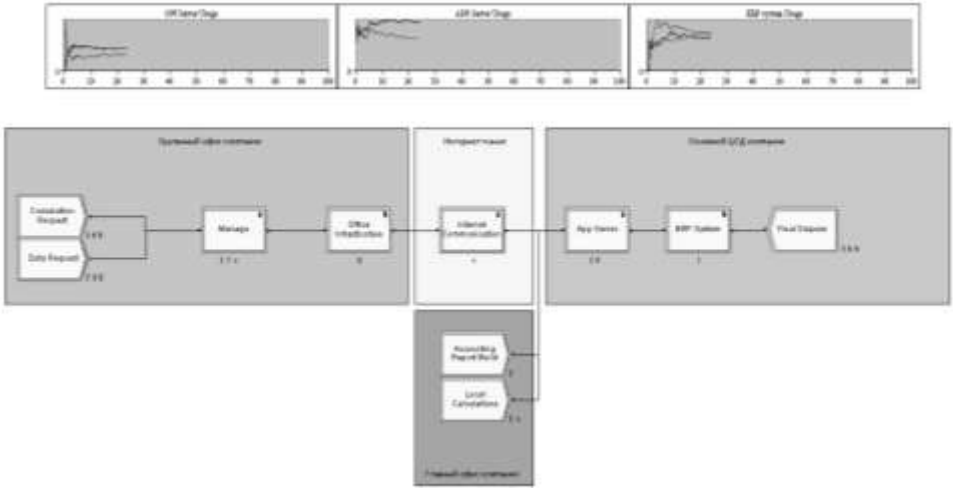


Рис. 1. Имитационная модель обработки заявок клиентов

Обработка обращения клиента (Manage)

Подмодель обработка обращения клиента будет состоять из 2 блоков Process (Предварительная беседа с клиентом, (Hello), Консультация клиента (Answer) и двух блоков Decide (Определение типа обращения (Ask)), у которого есть два выхода: да и нет. На выходе «да», осуществляется отправка заявки в систему, на выходе «нет» клиент отправляется на консультацию. И блока («Необходима работа с системой» (Is Know Answer)), на выходе «Да» которого клиент выходит из модели, а в обратном случае – заявка передается в работу.

На рис. 2 изображена подмодель «обработка обращения клиента».

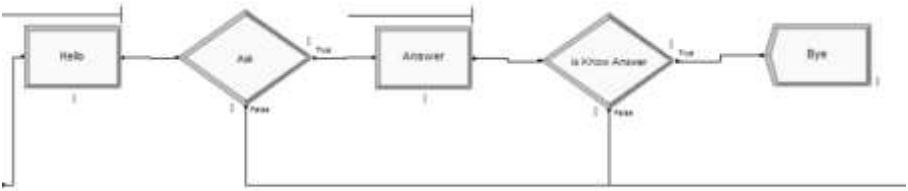


Рис. 2. Имитационная подмодель «Обработка обращения клиента»

Региональный офис (Office Infrastructure)

Подмодель Региональный офис будет состоять из 3 блоков Process (Работа локальной сети (LAN), Соединение по технологии VPN, Соединение по технологии RDP), 2 блока Assign (VPN и RDP), представляющих собой процесс идентификации трафика по типу и Блока

Decide (Определение типа подключения (Ask)), у которого есть два выхода: да и нет. На выходе «да», осуществляется подключение по технологии VPN, на выходе «нет» - RDP. На рис. 3 изображена подмодель «Региональный офис».

Каналы связи в сети Интернет (Internet Communication)

Подмодель Каналы связи в сети Интернет состоит из 3 блоков Process (Передача данных локальным провайдером Интернет (Local Provider), Передача данных основным провайдером Интернет ЦОД (MAIN Provider) и Передача данных резервным провайдером Интернет ЦОД (Reserve Provider)), блока Decide (Failsafe) для определения работоспособности основного провайдера. На рис. 4 изображена подмодель «Каналы связи в сети Интернет».

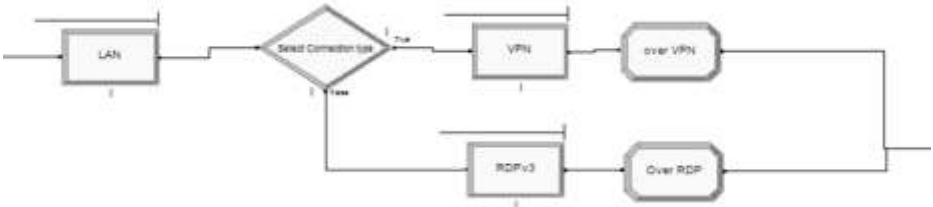


Рис. 3 Имитационная подмодель «Региональный офис»

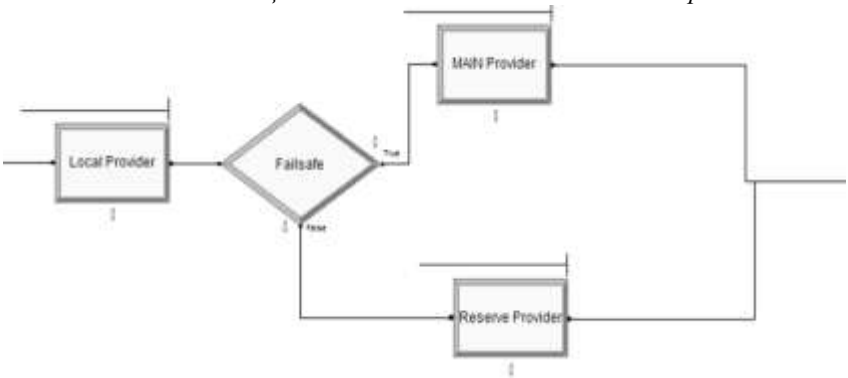


Рис.4. Имитационная подмодель "Каналы связи в сети Интернет"

Сервер приложений (App Server)

На рис. 5 изображена подмодель «Сервер приложений». Она состоит из 4 блоков Process:Процесс обработки доступа по технологии VPN; Процесс обработки доступа по технологии RDP; Сервер приложений 1; Сервер приложений 2; Трех блоков Decide: 1) Определение типа подключения (Внутренний-Внешний) 2) Определение технологии подключения (VPN/RDP) 3) Выбора назначенного сервера приложений (Server 1 / Server 2) 4)Выход из системы локальных вычислений.

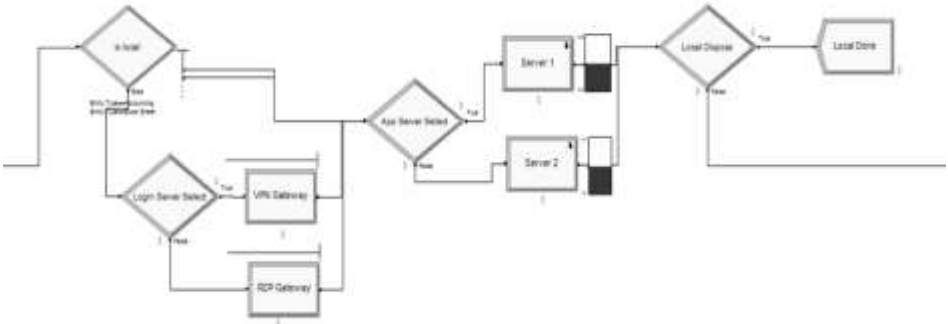


Рис. 5. Имитационная подмодель "Сервер приложений"

Система планирования ресурсов предприятия (ERP System)

На рис. 6 представлена подмодель «Система планирования ресурсов предприятия». Она состоит из одного блока Decide, олицетворяющего систему распределения нагрузки внутри ERP системы и трех блоков Process (AOS1, AOS2, AOS3), обозначающих сервера вычислений ERP системы.

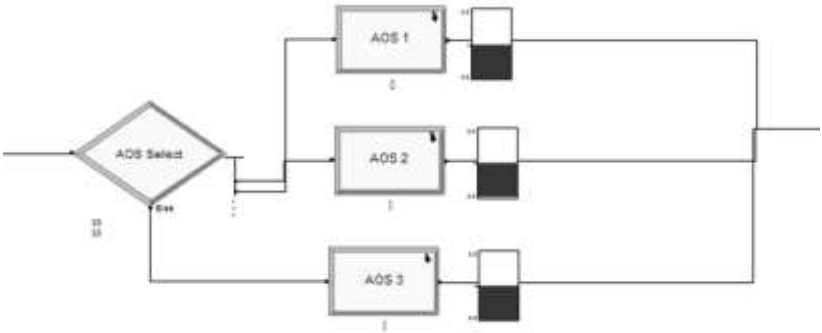


Рис. 6. Имитационная подмодель «Система планирования ресурсов предприятия»

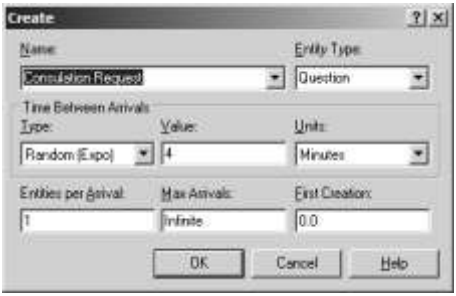


Рис. 7. Настройка блока генерации заявок от клиентов

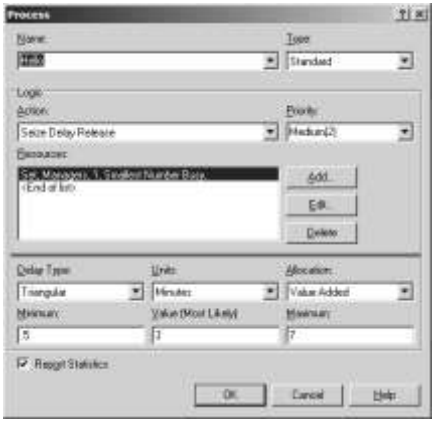


Рис. 8. Настройка процесса «Предварительная беседа с клиентом»

Рис. 9. Настройка блока «Определение типа обращения»

Далее переходим к заполнению блоков данными (временные параметрами). Двойным щелчком по блоку ***Consulation Request*** (Консультация) переходим в свойства (рис. 7).

Открываем подмодель «Обработка обращений клиентов». Двойным щелчком на блоке «Предварительная беседа с клиентом» переходим в свойства (рис. 8). Далее переходим на блок Decide («Определение типа обращения»). Транзакт, попадающий в блок, направляется в одну из 2 или N ветвей. Ветвление может быть условным (ветвь выбирается по некоторому условию) или вероятностным (заданы вероятности перехода в каждую из ветвей). Свойства данного блока представлены на рис. 9.

По аналогии заполняются остальные блоки модели обработки обращения клиентов. Временные параметры представлены в таб.1. Далее заполняем модули данных Entities (сущности) и Resource (ресурсы). Список Entities содержит все типы сущностей, которые присутствуют в модели. При появлении нового типа сущности в одном из блоков системы, данный тип сущности появляется и в общем списке. Список Resource содержит все ресурсы модели.

Третий шаг при разработке имитационной модели - настройка модели. На данном этапе мы рассмотрим такие показатели: время выполнения, количество имитаций, настройка анимации.

Время выполнения имитации составит 27 рабочих дней (месяц), один рабочий день равен 24 часам. Количество имитаций – 5. Настройка анимации представляет собой внесение в рабочую область Arena графических рисунков. Окно настройки временных параметров представлено на рис. 10.

Рис. 10. Настройка временных параметров модели

На этапе отладки модели можно запустить модель в нужном темпе и посмотреть анимацию движения документов и работы персонала. Этап тестирования заключается в проведении имитаций и сравнении выданных данных с реальными показателями работы организации. В нашем случае все показатели были близкими к существующим на данный момент времени показателям работы офиса.

После выполнения имитационной модели, Arena автоматически сгенерирует отчеты. Программный комплекс предоставляет следующие виды отчетов: краткий обзор категорий, сущности, процессы, очереди и ресурсы. Далее мы проанализируем наиболее значимые показатели данных отчетов.

Время выполнения имитации – 27 рабочих дней. Один рабочий день составит 16 часов. В офисе работают три менеджера, один руководитель офиса и один новичок. В распоряжении офиса находятся два и более переносных или настольных компьютеров, телефон, факс, сетевое оборудование.

В нашем случае среднее время на составление коммерческого предложения (VA Time) оказалось равным 26 минутам, наименьшее время обслуживания — около 13.4 минут, наибольшее — около 172.60 минут. Время необходимое для консультации клиента составило в среднем 19 минут, при наименьшем времени в 3 минуты и наибольшем – в 49 минут.

Время ожидания процесса создания коммерческого в очереди варьировалось от 0.00101891 минут до 147 и в среднем составило 9.2 минуты. Суммарное среднее время заявки, проведенное в очереди составляет 9.21 минут. Количество запросов, вошедших в систему за время имитации – 13,538 , количество обслуженных системой - 13,520.

Среднее время работы над коммерческим предложением оказалось равным 7 минутам, наименьшее время обслуживания — менее минуты, наибольшее — около 38 минут. Время ожидания составления КП имеет диапазон от 0 до 240 минут, среднее значение — 11 минут. Суммарное время, проведенное КП в системе — от 11 до 277 минут, в среднем 36 минут. Количество КП введенных в систему за время имитации – 41808 количество листов обработанных(составленных) за время имитации-41801

Соотношения количества всех сущностей в модели представлено на диаграмме (рис.11).

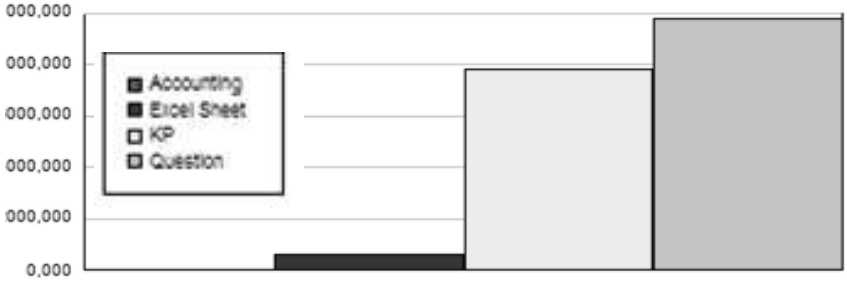


Рис. 11. Соотношение количества сущностей в модели

Сводные данные из отчета о сущностях представлены в табл. 3.

Таблица 3

Сводные характеристики сущностей в модели

Наименование транзакта	Кол-во тр.		Время обслуживания			Время ожидания			Суммарное время		
	In	Out	Min	Aver	Max	Min	Aver	Max	Min	Aver	Max
Расчет статистики	196	195	0	0,028	1,0	0,00	7,1179	223,67	10,4933	30,5891	244,20
Локальные вычисления	3572	3571	0	0,9823	7,0	0,00	1,8723	94,2407	18,7211	57,7187	157,67
Коммерческое предложение	41808	41801	0	7,2776	38,0	0,00	10,6667	248,23	11,6491	36,6964	277,87
Консультация	53099	53093	0	5,6571	21,0	0,00	2,6492	241,58	2,1136	22,4598	283,24

Сводные данные из отчета по ресурсам представлены в табл. 4.

Таблица 4

Параметры использования ресурсов в модели

Наименование ресурса	Коэф. использования	Число занятых ресурсов	Емкость ресурса	Количество захватов ресурса
AOS1 CPU	0,47	0,93	2,00	2 845,00
AOS2 CPU	0,43	0,87	2,00	2 745,00
AOS3 CPU	0,47	0,93	2,00	2 892,00
Cisco ASA	0,00	0,00	10,00	6 365,00
Интернет-канал	0,01	0,01	1,00	8 338,00
Новичок	0,12	1,22	10,00	5 674,00
Руководитель офиса продаж	0,17	1,73	10,00	7 867,00
Локальный интернет-канал	0,08	0,83	10,00	8 452,00
Сервер RDP CPU	0,23	0,23	1,00	6 380,00
Сервер VPN CPU	0,16	0,16	1,00	2 072,00
Менеджер	0,07	2,02	30,00	9 040,00
Резервный интернет-канал	0,01	0,01	1,00	114,00
RDP пул	0,01	0,33	30,00	2 088,00
Инфраструктура офиса	0,00	0,00	10,00	8 453,00
Server 1 CPU	0,68	1,36	2,00	5 246,00
Server 2 CPU	0,49	0,98	2,00	3 794,00

Соотношение количества всех ресурсов представлено на рис.12.

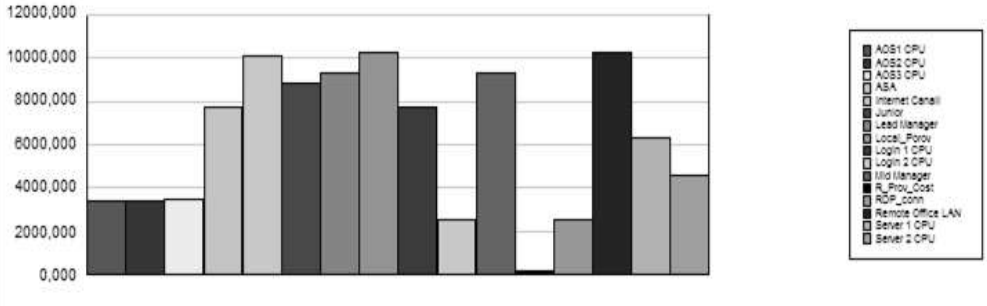


Рис. 12. Соотношение количества ресурсов, использующихся в модели

На основании приведенных данных в таблицах, можно сделать следующие выводы: в среднем в день менеджеры компании обрабатывают 267 консультаций, и 211 коммерческих предложений. Порядка 20

пользователей в день производят ресурсоемкие локальные вычисления, связанные с внутренними процессами, протекающими в компании. Данные процессы не были подробно рассмотрены в текущей работе но, несомненно, оказывают влияние на изучаемый бизнес-процесс. Каждые сутки автоматически запускается процедура создания отчетности.

В среднем на расчет коммерческого предложения самой системой уходит порядка 12 минут, остальное время тратится менеджером на проведение предварительного интервьюирования клиента (в среднем 14 минут) и на коммуникации внутри сетевого канала и канала сети интернет. На основе системного анализа применения информационных технологий в деятельности компании был определен перечень и характеристики факторов, влияющих на непрерывность функционирования ИТ-сервисов компании, а также – значения допустимых отклонений основных параметров, при которых обеспечивается требуемый уровень эффективности работы ИТ-сервисов.

В результате имитационного моделирования возможных причин сбоев в работе организации был выявлен ряд узких мест и единых точек отказа, снижающих общую непрерывность деятельности организации. Основным узким местом для бизнес-процесса СКП является региональный интернет канал. Как показало исследование сбои на интернет - магистралях региональных представительств происходят как минимум раз в месяц, тогда как интернет провайдер главного офиса представляет собой более крупную организацию и допускает сбои не чаще раза в год. При этом в главном офисе имеется резервный канал большей полосы пропускания, что позволяет бесперебойно продолжить работу в случае отказа главного интернет провайдера.

Исследование показало, что точки входа региональных представительств в инфраструктуру офиса не зарезервированы. В главном ЦОДе компании используется только один коммутатор Cisco ASA для доступа по технологии VPN и один сервер для обеспечения доступа по технологии RDP. При выходе из строя одного из этих устройств доступ сотрудников из вне-офиса по определенной технологии будет не возможен.

Серверы приложений главного офиса находятся в виртуальной форме, что практически исключает влияние физического сбоя оборудования на их работу, но в тоже время имеет место быть происхождения программного сбоя, способного нарушить бесперебойную работу системы. Пользователи определенным образом привязаны к серверам, что грозит отказом в доступе некоторой группе пользователей при выходе из строя одного из сервера. Автоматическое переключение не осуществляется.

Описанные выше уязвимости в системе обеспечения непрерывности бизнеса могут приводить к следующим потерям:

В случае отказа регионального провайдера интернет целый офис прекращает свою работу. В среднем, по результатам наблюдений, на устранение поломки на линии у сотрудников технической поддержки провайдера уходит от одного до трех часов. Это означает, что в среднем офис откажет в обслуживании двум клиентам с простыми вопросами и от одного до четырех клиентов с желанием получить коммерческое предложение. Если клиент еще не определился с выбором лизингодателя, отказ в обслуживании может негативно сказаться на имидже компании что за собой повлечет обращение к конкурентам и потери прибыли для компании.

В случае выхода из строя оборудования, предоставляющего доступ по технологии VPN около 75% региональных сотрудников будут испытывать проблемы с подключением. Аварии такого плана не происходили в компании за рассматриваемый период, поэтому оценить время, требуемое на восстановление удается только эмпирическим путем. Оно составит порядка 6 – 8 часов для обновления микрокода оборудования или 3-4 дня, для доставки нового предварительно настроенного оборудования в региональный офис.

По примерным расчетам при простое от 6 до 8 часов в обслуживании будет отказано от 1 до 3 клиентам в консультациях и от 5 до 7 клиентам в расчете коммерческого предложения, при выходе регионального оборудования. При выходе из строя маршрутизатора, расположенного в главном офисе, ни одно подключение по технологии VPN не сможет быть выполнено, что повлечет собой гораздо большие отказы в обслуживании на время ремонта оборудования, в размере до 70 обращений клиентов.

При возможном отказе сервера, обеспечивающего доступ по технологии RDP или сервера приложений, его перезагрузка займет около 5 минут, а восстановление из резервной копии при максимальной скорости чтения с ленты 1.7 TB/hr (LTO-4), займет порядка 40 минут. За это время произойдет отказ в обслуживании примерно двум клиентам.

После выполнения имитационного моделирования всех возможных угроз и выявления узких мест в программе обеспечения непрерывности деятельности организации, был выработан список указаний, рекомендуемых к выполнению для повышения общей катастрофоустойчивости бизнес-процесса организации:

Для предотвращения реализации полного риска отсутствия интернета в региональном офисе предлагается использование резервного интернет канала. В частности рекомендуется оснастить один из переносных компьютеров регионального представительства устройством

беспроводного доступа в интернет по технологии 3G или 4G. Устройство позволяет получать доступ к сети интернет в зоне покрытия радио сигнала, не зависимо от расположения, на требуемой для работы с системой скорости. Это позволит продолжить работу в аварийном режиме сниженной продуктивности при проблемах связанных с отсутствием интернета в региональном представительстве или отсутствия физического доступа в здание офиса, в случае возникновения какого-либо чрезвычайного происшествия. Сотрудники могут быстро переместиться в любое помещение и продолжить работу от батареи ноутбука в течении порядка двух часов или от сети электрического снабжения.

Так, как режим доступа в головной офис предлагает использование двух технологий VPN и RDP в активном режиме, то есть в зависимости от технической возможности пользователи подключаются по одной из выбранных технологий, это является узким местом для групп пользователей, сбой в технологии доступа которых произошел. Сама по себе технология RDP доступна всем сотрудникам и не требует никаких дополнительных специальных аппаратных средств, кроме персонального компьютера под управлением операционной системы Microsoft Windows XP SP3 и выше. Что наделяет ее свойством резервной по отношению к технологии VPN, доступ к которой возможен только сотрудникам организации при наличии специального устройства (маршрутизатора) или программного комплекса Cisco VPN client. Для поддержания бесперебойности работы, в случае выхода из строя технологии VPN, предлагается разработать и внедрить инструкцию по смене типа подключения для пользователей, работающих по VPN на RDP. В свою очередь для обеспечения двойной избыточности VPN-пользователей и одинарной избыточности пользователей технологии RDP рекомендуется произвести дублирование сервера шлюза и настройки программного обеспечения в режим кластера высокой доступности по технологии Active/Active. Этот режим позволяет равномерно распределять нагрузку по серверам, а в случае сбоя автоматически производить переключение на рабочий узел.

Сервера приложений главного офиса используются в первую очередь для подключения региональных сотрудников по технологии RDP, и некоторыми сотрудниками главного офиса для выполнения ресурсоемких задач. С целью равномерного распределения нагрузки между серверами пользователи были принудительно ограниченны к подключению на определенный сервер. Что означает что у конкретного пользователя есть право подключаться только на один из двух серверов. При выходе из строя которого пользователь получает отказ в обслуживании. Предлагается в замен ручного распределения вычислительных ресурсов использовать автоматические технологии вычислительного кластера.

Кластер — это группа из двух или более серверов, действующих совместно для обеспечения безотказной работы набора приложений или служб и воспринимаемых клиентом как единый элемент. Узлы кластера объединяются между собой с помощью аппаратных сетевых средств, совместно используемых разделяемых ресурсов и серверного программного обеспечения. Microsoft Windows Server 2003/2008 поддерживает две технологии кластеризации: кластеры с балансировкой нагрузки (Network Load Balancing) и кластеры серверов. В первом случае (кластеры с балансировкой нагрузки) служба Network Load Balancing придает службам и приложениям свойства высокого уровня надежности и масштабируемости за счет объединения до 32 серверов в единый кластер. Запросы от клиентов в данном случае распределяются среди узлов кластера прозрачным образом. При отказе узла кластер автоматически изменяет свою конфигурацию и переключает клиента на любой из доступных узлов. Этот режим конфигурации кластера также называется active-active режимом, когда одно приложение работает на нескольких узлах.

Кластер серверов распределяет свою нагрузку среди серверов кластера, причем каждый сервер несет свою собственную нагрузку. Если происходит отказ узла в кластере, то приложения и службы, настроенные на работу в кластере, прозрачным образом перезапускаются на любом из свободных узлов. Кластеры серверов используют разделяемые диски для обмена данными внутри кластера и для обеспечения прозрачного доступа к приложениям и службам кластера. Для них требуется специальное оборудование, но данная технология обеспечивает очень высокий уровень надежности, поскольку сам кластер не имеет какой-либо единственной точки отказа. Этот режим конфигурации кластера также называется active-passive режимом. Приложение в кластере работает на одном узле с общими данными, расположенными на внешнем хранилище.

Таким образом, моделирование и методы имитационного моделирования представляют собой возможность для разработки, оценки и модернизации планов обеспечения непрерывности бизнеса без ущерба для текущих операций. Кроме того, из-за наличия графических пользовательских интерфейсов, компьютерное моделирование представляет собой ценный инструмент для обучения и подготовки участников бизнес-процессов. Сочетание графических пользовательских интерфейсов и анализа сценариев обеспечивает комплексные и разносторонни возможности для поддержки принятия решений. В нашем исследовании мы рассматриваем использование ИМ в качестве части комплексной интегрированной функционально-имитационной модели обеспечения непрерывности бизнеса.

В ходе исследования построена имитационная модель критически важных бизнес-процессов организации. Производя имитационные эксперименты с использованием различных наборов деструктивных факторов в комбинации с мерами, снижающими уязвимость системы и препятствующими возникновению угроз непрерывности бизнес-процессов, вычислялись ключевые показатели эффективности бизнес-процессов, а также производилась индикация критических элементов инфраструктуры, разрабатывались рекомендачии по совершенствованию существующей СУНБ.

Публикация выполнена в рамках проекта РГНФ № 11-06-01006 «Разработка и апробация модели подготовки научно-педагогических кадров к обеспечению информационной безопасности в ИКТ-насыщенной среде».

Библиографический список

1. Петренко С. А. Управление непрерывностью бизнеса. Ваш бизнес будет продолжаться. Информационные технологии для инженеров. - М.: ДМК Пресс, 2011. - 400 с.

2. Чусавитин М.О. Применение ИТ-решений при управлении непрерывностью бизнеса// Современные информационные технологии и ИТ-образование: Сбор. избр. тр. VII Междунар. науч. практ. конф. Под ред. проф. В.А. Сухомлина. - М.: ИНТУИТ.РУ. С. 635-642.

3. Чусавитин М.О. Применение методов имитационного моделирования при управлении непрерывностью бизнеса //Труды Вольного экономического общества России. Том сто шестьдесят четвертый. М. Российский экономический университет имени Г.В. Плеханова, 2011. – Т. 164. С. 192—200.

4. Чусавитин М.О. Использование средства ARENA при моделировании нарушения непрерывности деятельности ИТ-инфраструктуры организации // Разработка инновационных механизмов повышения конкурентоспособности выпускников ИТ-специальностей вуза в условиях моно промышленного города: (сб. ст.)/ под ред. Г.Н.Чусавитиной, Л.З. Давлеткиреевой. - Магнитогорск: МаГУ, 2012. – 160 с. – С.141-151 (ISBN 978-5-86781-982-8).

***М.О. Чусавитин**, аспирант*
Г.Н .Чусавитина, *к.п.н., профессор кафедры информационных технологий*

АНАЛИЗ ПРОБЛЕМЫ ГОТОВНОСТИ ПЕДАГОГИЧЕСКИХ КАДРОВ К ПРОФИЛАКТИКЕ И ПРОТИВОДЕЙСТВИЮ ИДЕОЛОГИИ КИБЕРЭКСТРЕМИЗМА СРЕДИ МОЛОДЕЖИ

ФГБОУ ВПО «Магнитогорский государственный университет»

Аннотация

В статье освещаются результаты проведённого исследования по анализу состояния проблемы подготовки педагогических работников к профилактике и противодействию идеологии киберэкстремизма.

Среди всех асоциальных явлений, представляющих угрозу национальной безопасности страны, особое место занимает молодёжный экстремизм. В России юридическое определение того, какие действия считаются экстремистскими, содержится в статье 1 Федерального Закона № 114-ФЗ «О противодействии экстремистской деятельности» (в ред. № 404-ФЗ от 28.12.2010 г.). Под экстремистской деятельностью (экстремизмом) понимается деятельность общественных и религиозных объединений, иных организаций, средств массовой информации, физических лиц по планированию, организации, подготовке и совершению действий, направленных на насильственное изменение основ конституционного строя, подрыв безопасности Российской Федерации, захват или присвоение властных полномочий, создание незаконных вооруженных формирований, осуществление террористической деятельности, унижение национального достоинства; пропаганда и публичное демонстрирование нацистской атрибутики или символики либо атрибутики или символики, сходной с нацистской атрибутикой или символикой до степени смешения; публичные призывы к осуществлению указанной деятельности или ее финансирование.

В условиях глобальной информатизации общества возрастают угрозы новой формы проявления экстремизма– электронного экстремизма или, как его часто еще называют, киберэкстремизма. Киберэкстремизм - это новая форма экстремизма, использующая для достижения своих целей компьютеры и электронные сети, новейшие коммуникационные технологии. По своему механизму, способам совершения и сокрытия киберэкстремисткая деятельность имеет определенную специфику, характеризуются высоким уровнем латентности и низким уровнем раскрываемости. Широкомасштабное внедрение информационно-коммуникационных технологий (ИКТ) представляет потенциально благоприятное поле для экстремисткой и террористической деятельности. При этом ИКТ используются экстремистами, с одной сто-

роны, как мощное средство в целях пропаганды своих взглядов, нагнетания обстановки напряженности, страха и т.д, а с другой стороны, ИКТ являются объектами террористических атак (разрушение объектов информационной инфраструктуры. нарушение безопасности информации).

В отечественной литературе выделяются достаточно условные основные формы проявления экстремизма: политический, национальный и религиозный. Экстремизм политический представляет собой деятельность, направленную на насильственное изменение политического строя или политики государства. Национальный экстремизм разжигает ненависть между нациями и народностями, пропагандирует неприятие людей не своей национальности, защиту «своего народа», его экономических интересов, культурных ценностей, национального языка и т. д. в ущерб представителям других национальностей. Религиозный экстремизм – нетерпимость к представителям той же или других религий.

В ряде стран (США, Китай, Россия, государства ЕС) созданы ведомствапо противодействию киберэкстремизму и терроризму. Крайним проявлением киберэкстремизма является кибертерроризм. Сам термин «кибертерроризм» появился в лексиконе предположительно в 1997 г. когда, тогда специальный агент ФБР, Марк Поллитт определил этот вид терроризма как «преднамеренные политически мотивированные атаки на информационные, компьютерные системы, компьютерные программы и данные, выраженные в применении насилия по отношению к гражданским целям со стороны субнациональных групп, или тайных агентов»[1]. Исследователи М. Дж. Девост, Б. Х. Хьютон, Н. А. Поллард определяют информационный терроризм (а кибертерроризм является его разновидностью) как: соединение преступного использования информационных систем с помощью мошенничестваили злоупотреблений с физическим насилием, свойственным терроризму; и сознательное злоупотребление цифровыми информационными системами, сетями или компонентами этих систем или сетей в целях, которые способствуют осуществлению террористических операций или актов [5].

В современном мире кибертерроризм тесно сращивается с киберпреступностью. Проблемы киберпреступности и кибертерроризма рассматриваются в научных работах Я. Александера, Д. Вертона, А. Джонсона, В.Замкового, А. Кампена, А.И. Примакина, В.Е. Кадулина, А. Коларика, Р. Ленхарда, Д. Лонсдале, Шафрански, Л. Янцевски и ряда других.

Вопросами информационной безопасности (ИБ), информационных войн и информационного оружия в исследованиях Л. Абаева, Д. Балуева, Д. Бородинова, В. Голубева, Г. Грачева, С. Гриняева, В. Дан-

чеева, С. Зелинского, Л. Земляновой, С. Кара-Мурзы, А. Клименко, Н. Кузьменка, А. Куликова, Г. Малинецкого, А. Московского, М. Мудави, С. Погодина, В. Потехина, Н. Потрубача, Е. Сатановского, А. Спивакова, Е. Старостиной, Д. Тренина, Т. Тропиной, О. Хохлышевой, В. Цыгичко, А. Щетилова, И. Юркина, А. Юрчишиной и др. Социально-философским проблемам информационных и психологических войн, атакже ИБ большое внимание в своих исследованиях уделяют ученые В.А. Братчиков, А.И. Воеводин, В.А. Галатенко, Г.В. Грачев, В.Г. Крысько, К.К. Колин и др.

Проблемы информационного насилия, в том числе насильственного воздействия Интернет-технологий на индивида и общество рассматривают О.Н. Арестова, Л.Н. Бабанин, А.Е. Воскунский, Н.А., Борщев, А. Купер, О.К. Тихомиров, Дж. Сулер, К. Хефнер и др. Исследованию социальных аспектов информатизации, в целях создания условий для развития информационной сферы российского общества, формирования его новой информационной культуры, атакже права, морали, нравственности, этики, адекватных условиям глобального информационного общества, посвящены исследования И.В. Роберт, К.К. Колин, И.В. Соколоваи др.

Теорию информационной и компьютерной этики разрабатывают Дж. Мур, Д. Джонсон, Дж. Снэппер, У. Бетчел, Л. Флориди, и др. Различные аспекты этико-правового характераИКТ отражены в работах И.Л. Галинской, А.И. Панченко, Дж. Снэппера, О.М Цыденовой и др. Среди отечественных исследований связанных с обеспечением информационно-психологической безопасности личности с целью предотвращения или нейтрализации негативных информационно-психологических воздействий можно выделить работы Э.М. Андреева, А.Е. Войскунского, А. Егорова, К.К. Колин, В.Е. Лепского, Г.Ю. Маклакова, А.В. Миронова, О.В. Смыслова, М. Эпштейн и др). Среди зарубежных труды С. Кинга, С. Томпсена, В. Бреннера, О. Эггераи М. Раутерберга, Т. Белсэйр, Дж. Морэйхэн-Мартина, П. Шумейкера, Ч. Чу, Дж. Сулера, К.С. Янг, Д. Гринфилда, К. Сурратт и др.

Правовое регулирование антикиберэкстремисткой деятельности основывается на федеральных законах «О связи», «Об информации, информатизации и защите информации», «О СМИ», ФЗ № 35-ФЗ от 16.03.2006г. «О противодействии терроризму» (в ред. № 404-ФЗ от 28.12.2010г.) и № 114-ФЗ от 25.07.2002г. «О противодействии экстремисткой деятельности» (в ред. № 54-ФЗ от 29.04.2008г.). Борьбас экстремизмом в интернете ведется с использованием соответствующих норм в уголовном законодательстве: о призывах к экстремистской деятельности (ст. 280 УК), возбуждении ненависти (ст. 282 УК), а также о публикациях, которые могут быть отнесены к деятельности экстремистского сообщества(ст. 282.1 УК) или запрещенной организации (ст.

282.2 УК). Также используются нормы КоАП:ст. 20.3 «Пропагандаи публичное демонстрирование нацистской атрибутики» и ст. 20.29 «Производство и распространение экстремистских материалов». 1 ноября 2012 г. вступил в силу закон «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию и отдельные законодательные акты Российской Федерации». Новый закон предусматривает создание «Единого реестра доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено». Помимо сайтов с порнографической информацией, пропагандой наркотиков, психотропных веществ и самоубийств, тудавойдет и информация, запрещенная к распространению в Российской Федерации как экстремистская.

Активную борьбу с проявлениями киберэкстремизма ведут правоохранительные органы. В материалах доклада Правозащитного Центра«СОВА» «Виртуальный антиэкстремизм. Об особенностях применения антиэкстремистского законодательствав Интернете (2007–2011)» (http://www.sova-center.ru/racism-xenophobia/publications/2012/09/d25322/) отмечается, что в 2007 году были известны всего три приговорапо уголовным делам за пропаганду в интернете (из 28 приговоров по ст.ст. 280 и 282 УК в целом), а в 2011 году их было вынесено не менее 52 (из 78). Наряду с правоохранительными органами, с киберэкстремизмом в России борются и общественные организации такие как Фонд «Дружественный Рунет» и Центр безопасного Интернета.

Проблема молодежного экстремизма в России, при сегодняшних темпах его развития, может занять в ближайшем будущем одно из лидирующих мест среди негативных социальных явлений. Вместе с тем, на наш взгляд, существуют целый ряд не решенных проблем, связанных с исследованием и предотвращением экстремистских преступлений совершаемых молодыми людьми в условиях информационного общества. Констатируя активную разработку различных аспектов превенции делинквентного поведения молодежи в ИКТ-насыщенной среде, мы пришли к выводу о том, что существует проблема определяющаяся противоречием, с одной стороны, между возросшей необходимостью в информационном обществе предупреждения такого опасного социального явления как экстремизм, и, с другой стороны, недостаточной степенью подготовки научно-педагогических кадров к профилактике и противодействию идеологии киберэкстремизма среди молодежи.

Актуальность проблемы обусловлена: 1) опасностью киберэкстремизма для общественно-го порядка, тенденцией перерастания данного асоциального явления в более серьезные преступления, такие как

терроризм, причинение тяжких телесных повреждений, массовые беспорядки и др.; 2) ростом количества экстремистских проявлений в статистике правонарушений совершаемых молодежью в глобальной сети Интернет; 3) возрастающей ролью системы образования как социального института имеющего возможность положительно влиять на снижение уровня преступлений киберэкстремисткой направленности за счет формирования личности индивидуума в процессе воспитания толерантности, культуры межэтнического общения; 4) недостаточной теоретико-методологической разработанностью оснований подготовки, повышения квалификации и переподготовки научно-педагогических кадров в данной области; 5) недостаточной представленностью психолого-педагогической проблематики профилактики киберэкстремизма в молодежной среде в спектре научных исследований научных психологических и педагогических школ.

Цель проводимого нами исследования сформулирована следующим образом - разработка и апробация модели подготовки студентов педагогических специальностей университета к профилактике и противодействию идеологии киберэкстремизма среди молодежи.

Научная новизна:

1. Определено содержание категории «профилактика и противодействие идеологии киберэкстремизма среди молодежи».

2. Обоснована и разработана концепция, модель и педагогическая технология формирования компетентности специалистов в области обеспечения профилактики и противодействия идеологии киберэкстремизма среди молодежи как одной из целей и результата развития культуры информационной безопасности.

3. Определены и разработаны основные направления практики, совместное действие которых обеспечивает эффективность подготовки научно-педагогических кадров профилактике и противодействию идеологии молодежного экстремизм в ИКТ-насыщенной среде.

Решение поставленной задачи планируется осуществлять с помощью комплекса методов: теоретических (аналитико-синтетический анализ; системный анализ; аналогия; моделирование); эмпирических (включенное наблюдение; анкетирование; интервьюирование; диагностирование; изучение и обобщение педагогического опыта; модуляция процессов, проявлений взаимозависимых характеристик, их апробация в естественных условиях образовательной практики). В процессе исследования найдут применение праксиметрические методы; структурно-генетический метод; педагогический эксперимент; методы математической статистики и информационных технологий (выявление статистических зависимостей; корреляционный анализ; компьютерно-статистическая обработка данных; графическое отображение результатов) методология интеллектуального анализа данных, методология

быстрой разработки приложений RAD и др. Для решения поставленных задач используются следующие основные научные подходы: системный, комплексный, процессный, деятельностный, ситуационный, личностно- ориентированный, компетентностный.

На факультет информатики ФГБОУ ВПО «МаГУ» накоплен определенный опыт в этом направлении. С 2008 года ведется работа по профилактике киберэкстремизма и терроризма среди молодежи. Тема «Кибепреступления» включена в читаемые дисциплины «Информационная безопасность», «Теория информационной безопасности и методология защиты информации», «Информационная безопасность и защита информации», «Информационная безопасность в системе открытого образования» и др. для студентов всех факультетов МаГУ. Студенты под руководством преподавателей участвуют в научно-исследовательской работе по данной проблеме. Регулярно принимают участие в круглых столах, семинарах, во всероссийских и международных конкурсах (IT-Security Conference for the Next Generation, «Обучение для будущего» корпорации «Прожект Хармони, Инк.», США; Министерство образования и науки Челябинской области и др.). Так в феврале 2010 года студентами факультета (Бешенцевой М.С., Сафаргалеевой Л.Ф., Фахриевым А.В.) был разработан учебный проект для студентов высших учебных заведений по противодействию кибертерроризму, который стал лауреатом международного конкурса ITSecurity Conference for the Next Generation проводимого Лабораторией Касперского. Преподаватели и студенты факультета информатики прошли стажировку в Институте проблем информационной безопасности Московского государственного университета имени М.В. Ломоносова(октябрь-ноябрь, 2008), где участвовали в Первой Всероссийской научно-практической конференции «Формирование устойчивой антитеррористической позиции гражданского общества как основы профилактики терроризма» и IV Международной конференции по проблемам безопасности и противодействия терроризму.

Исследования по названной тематике, проводимые студентами и преподавателями, поддерживаются различными гранами:

- «Построение модели компетенций учителя в области профилактики негативного влияния ИКТ» (Конкурс исследовательских проектов на2007 год для студентов, аспирантов, молодых учёных вузов Челябинской области; 06 - Общественные и гуманитарные науки; Челябинский научный центр УрО РАН, № 070.06.01-07.БХ);

- «Активизация учебно-воспитательной работы со школьниками по преодолению негативного воздействия информационно-коммуникативной среды» (Региональный конкурс 2007 г. Российского государственного научного фонда«Урал: Челябинская область», № 07-06-85614 а/У);

- «Управление рисками, порождаемыми применением информационно-коммуникативных технологий в образовательном процессе вуза»(РГНФ, Информационная деятельность в области образования и педагогики; 2008-2009, № 08-06-00166а);

- Организационно-техническое обеспечение проведения всероссийской научной школы для молодежи «Управление информационными ресурсами образовательных, научных и производственных организаций» (Федеральная целевая программа«Научные и научно- педагогические кадры инновационной России» на2009-2013 годы, Федеральное агентство по науке и инновациям; 20.00.00 Информатика, 2009, Государственный контракт № 02.741.11.2082) и др.

Факультет информатики участвует в проектах академического сотрудничества с поставщиками программного обеспечения по защите информации – «Digital Security», Лабораторией Касперского, MSDN Academic Alliance, SearchInform, CA и др.

В ходе выполнения НИР планируется:

- исследование и систематизация проблемы обеспечения кибербезопасности;

- обоснование и разработка концепции, модели и педагогической технологии формирования компетентности специалистов в области обеспечения профилактики и противодействия идеологии кибеэкстремизма;

- апробация разработанной концепции в процессе научной и профессиональной подготовки молодых специалистов, в том числе и студентов педагогических специальностей вузов, в системе профессиональной переподготовки и повышения научной квалификации;

- использование результатов научного исследования в образовательном процессе;

- вовлечение учреждений и организаций системы науки и образования субъектов РФ в освоение результатов проекта.

Теоретическая значимость исследования заключается в разработке методологии формирования компетентности молодежи, педагогических кадров в вопросах профилактики и противодействию идеологии киберэкстремизма как одной из целей и результата развития культуры информационной безопасности. Результаты исследования углубляют разрабатываемую в научной теории проблему развития информационной культуры современного специалиста; организационных, правовых и программно- технических аспектов проблемы обеспечения ИБ.

Практическая значимость исследования заключается в создании комплексного научно-методического обеспечения процесса формирования компетентности молодежи в сфере профилактики и противодействию идеологии киберэкстремизма, включающего: 1) учебные посо-

бия и методические рекомендации; 2) оценочно-критериальный инструментарий мониторинга; 3) программы авторских спецкурсов и спецсеминаров для студентов, преподавателей вузов, молодых ученых и аспирантов, учителей и учащихся общеобразовательных школ.

Материалы исследования могут использоваться при модернизации действующих учебных планов и программ подготовки аспирантов, молодых ученых, студентов, учителей, учащихся общеобразовательных школ, разработке и организации спецкурсов, спецсеминаров, элективных курсов, проведении научных школ, конференций.

Исследование выполняется в рамках проекта№ 13-06-00156 «Подготовка педагогических кадров к профилактике и противодействию идеологии киберэкстремизма среди молодежи» поддержанного РГНФ.

Библиографический список

1. Rrasavin S. What is Cyber-terrorism?// http://rr.sans.org/infowar

2. Зеркина (Чернова) Е.В., Чусавитина Г.Н. , ИКТ: инновация небезопасная, // Народное образование. 2008. № 8.С. 273 – 276.

3. Зеркина Е.В., Чусавитина Г.Н. Подготовка будущих учителей к превенции девиантного поведения школьников в сфере информационно-коммуникативных технологий. – Магнитогорск: МаГУ, 2008. – 184 с.

4. Зеркина Е.В., Чусавитина Г.Н. Проблемы организации учебно-воспитательной работы со школьниками в целях нейтрализации негативного воздействия ИКТ// Вестник МГОУ. М. 2006, – С. 100 – 105.

5. Томас Тимоти Л. Сдерживание асимметричных террористических угроз, стоящих перед обществом в информационную эпоху // Мировое сообщество против глобализации преступности и терроризма: матер. междунар. конф. М., 2002. – С. 165.

6. Чусавитин М.О. Управление рисками безопасности образовательно-информационной среды с использованием Digital Security Office // Материалы XIX Международной конференции «Применение новых технологий в образовании». Троицк, 2009. – С. 518 – 521.

7. Чусавитин М.О. Модель активизации учебно-воспитательной работы со школьниками по нейтрализации негативного воздействия информационно-коммуникативной среды // Информационная безопасность в открытом образовании : Сб. материалов науч. практ. конф. МаГУ. Магнитогорск, 2007. – С. 96 – 99.

8. Чусавитина Г.Н. Автоматизация оценки уровня защищенности информационных ресурсов образовательного учреждения С учетом стандартов ISO 17799:2005 и ISO 27001// Информационная

безопасность региона: гуманитарные и технические аспекты: сб. материалов Второй всерос. науч. практ. конф. Екатеренбург, 2009. – С. 249 – 252.

9. Чусавитина Г.Н. Информационная безопасность в открытом образовании// Информационная безопасность в открытом образовании. Магнитогорск, 2011. – С. 5 – 10.

10. Чусавитина Г.Н. Применение интегративных механизмов при подготовке будущих учителей в области обеспечения информационной безопасности // Вестник компьютерных и информационных технологий, № 5, 2010. - С. 49-54.

11. Чусавитина Г.Н. Развитие компетенций научно-педагогических кадров по обеспечению информационной безопасности в ИКТ-насыщенной среде// Спрос и предложение на рынке труда и рынке образовательных услуг в регионах России : сб. докладов по материалам VIII всерос. науч.практ. Интернет- конф. Петрозаводск, 2011. – С. 338 – 345.

12. Чусавитина Г.Н. Чусавитин М.О. Организационно-педагогические механизмы формирование общекультурной компетенции в сфере информационной безопасности у студентов педагогических специальностей вузов. – Вятка: ФГБОУ ВПО «Вятский государственный гуманитарный университет», 2012.

13. Чусавитина Г.Н. Элективный курс «Основы информационной безопасности» // Информатика и образование. 2007. № 4. – С.43 – 56.

14. Чусавитина Г.Н., Чернова Е.В. Толерантность как средство борьбы с экстремизмом и терроризмом // Современные проблемы науки и образования: тезисы докл. XLIII внутривуз. науч. конф. преп. МаГУ. – Магнитогорск. 2011. – С. 100 – 102.

15. Чусавитина Г.Н., Чусавитин М.О. Анализ безопасности образовательно-информационной среды вуза и управление рисками // II Всероссийская научно-практическая конференция «Информационная среда ВУЗаXXI века» »: Сборник трудов участников конференции. Петрозаводск, 2008. – С. 159 – 162.

16. Чусавитина Г.Н., Чусавитин М.О. Подготовка будущих учителей в области обеспечения информационной безопасности в системе открытого образования // Сборник трудов участников международного научно-практического семинара. 2008. – С.169 – 181.

Научное издание

Под редакцией
Чусавитиной Галины Николаевны
Давлеткиреевой Лилии Зайнитдиновны
Черновой Елены Владимировны

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ВОПРОСЫ ПРОФИЛАКТИКИ КИБЕРЭКСТРЕМИЗМА СРЕДИ МОЛОДЕЖИ

Печатается в авторской редакции

Подписано в печать 13.05.2013 г.
Формат 60x84 1/16. Усл. печ. л. 9,30. Уч.-изд. л. 8,89.
Тираж 100 экз. Заказ № 166. Цена свободная
Издательство Магнитогорского государственного университета
455038, г. Магнитогорск, пр. Ленина, 114
Типография ООО «Бизнес Поставка»
455028 Челябинская область, г. Магнитогорск, ул. Набережная, 10.