УДК 004.056.52

МЕХАНИЗМЫ ПРОТИВОДЕЙСТВИЯ КИБЕРЭКСТРЕМИЗМУ И КИБЕРТЕРРОРИЗМУ В СИСТЕМЕ ОБРАЗОВАНИЯ

Макашова В.Н.

ФГБОУ ВПО «Магнитогорский государственный университет», Магнитогорск, e-mail: makashova.vera@mail.ru

Актуальность темы обусловлена широким применением современных информационных технологий в образовательных учреждениях и повышением требований к содержанию Интернет-контента. В статье описаны механизмы противодействия различным угрозам, в том числе идеологии киберэкстремизма и кибертерроризма. Приведены ссылки на основные законы РФ, регламентирующие содержание открытого Интернет-контента и принципы хранения и передачи персональных данных. Рассмотрены основные механизмы обеспечения информационной безопасности образовательного учреждения (фильтрация и мониторинг) как с точки зрения входящего потока данных, так и исходящего. Даны рекомендации по применению программных продуктов, обеспечивающих информационную безопасность, для различных конфигураций аппаратных средств образовательных учреждений. Затронуты вопросы просвещения родителей и учащихся. Выявлена проблема недостатка квалифицированных кадров, осуществляющих управление политикой информационной безопасности образовательных учреждений.

Ключевые слова: информационная безопасность, фильтрация контента, мониторинг контента, киберэкстремизм

MECHANISMS TO COUNTER CYBER EXTREMISM AND CYBER TERRORISM AT EDUCATIONAL INSTITUTIONS

Makashova V.N.

Magnitogorsk State University, Magnitogorsk, e-mail: makashova.vera@mail.ru

The widespread use of Internet technologies at educational institutions has created a need for the strict control of the Internet content. The information age has brought to the world, not only the widespread development of technology and computerization of all life, but also led to the emergence of a form of social deviance as kibeprestupnost, which is now gaining wider development. Hacks electronic banking network, propaganda war, extremism on the Internet , attacks on government websites – this is not a complete list of what often turns to states and individuals information age. Cyber-terrorism is a new form of terrorism, which is to achieve its goals of terrorist use of modern information technology. In its mechanism, methods to commit and conceal such crimes are characterized by high latency, low levels of detection and cause incomparably greater harm than the crime «in the real world» as its purpose have damage and incapacitation of critical infrastructure, information and blackmail perpetrated remotely. Cyber-terrorism – is a serious threat to humanity. The experience that already exists in the international community in this area supposedly shows undeniable vulnerability of any state, especially as cyber terrorism has no borders and age limits. Cyber-terrorists can be equally threatening information systems located virtually anywhere in the world. How can you resist kiberekstremizmu how to prepare the younger generation to live in a sea of global information and do not drown in it? Consider the basic countermeasures to cyber terrorism: the control of the state and society, and countermeasures that are used directly in the educational institutions.

Keywords: Information safety, content filtering, content monitoring, cyber extremism

Глобальные процессы информатизации современного общества и образования обусловливают существенное обострение проблем информационной безопасности.

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 важнейших объектов инфраструктуры, информационный шантаж и совершаются удаленно.

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 и возрастных рамок. Кибертеррорист способен в равной степени угрожать информационным системам,

расположенным практически в любой точке земного шара.

К причинам, порождающим экстремистские настроения в 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 [2]. Наиболее полно, на наш взгляд, совокупность причин молодежного экстремизма в России обозначил С.Н. Фридинский, 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. Как можно противостоять киберэкстремизму, как готовить подрастающее поколение жить в море глобальной информатизации и не утонуть в нем?

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

Рассмотрим основные меры противодействия кибертерроризму: контроль со стороны государства и общества и механизмы противодействия, используемые непосредственно в образовательных учреждениях.

Территориальные органы Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзора) осуществляют контроль образовательных учреждении на предмет соблюдения законодательства. Для образовательных учреждений особо важными являются № 152-ФЗ «О персональных данных» и № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»

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 [3]. Для всех образовательных учреждений характерно наличие баз данных с информацией об учащихся: фамилия, имя, отчество, дата рождения, место рождения, адрес проживания, контактные телефоны родителей учащихся (законных представителей), сведения об учебном процессе и занятости обучающегося (перечень изученных, изучаемых предметов и факультативных курсов), успеваемость, в том числе результаты текущего контроля успеваемости, промежуточной и итоговой аттестации, данные о посещаемости уроков, причины отсутствия на уроках, поведение в школе, награды и поощрения и др. Необходимо отметить, что наряду с общеобразовательными учреждениями существуют специальные коррекционные образовательные учреждения, для полноценной работы которых в базах данных имеется дополнительная информация: диагноз, схемы лечения, Ф.И.О. медицинского персонала и т.д.

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.

В последнее время количество детей и подростков, получающих возможность выходить в интернет из дома или с помощью мобильных средств коммуникаций, существенно увеличивается, а их возраст уменьшается. В процессе обучения современные школьники активно использует пространство Интернет. При этом мы уже отметили, что всемирная информационная сеть – это не только хранилище ценной и разнообразной информации, благодаря которой можно решать образовательные задачи, но и источник разнообразных киберугроз. Изначально интернет развивался вне какого-либо контроля, поэтому сейчас он представляет собой огромную базу информации, причем далеко не всегда безобидной. Следует понимать, что подключаясь к сети Интернет, школьники могут получить доступ к нежелательному содержимому, совершать неконтролируемые покупки, инициировать контакты с незнакомыми людьми с помощью чатов или электронной почты, скачивать зараженные вредоносным ПО программы и т.д. К сайтам нежелательным для детей относятся сайты, которые дети не должны посещать по возрастным ограничениям: жестокие игры, онлайновые казино, порнография, сайты, пропагандирующие насилие, сайты сексуальных меньшинств, сайты магазинов интим-услуг, сайты, разжигающие расовую дискриминацию, сайты террористов и т.п.

В последнее время в России обостряется проблема молодежного киберэкстремизма, обусловленная рядом факторов: это становление и развитие российского терроризма и экстремизма на весьма благоприятном криминогенном фоне; рост ИКТ-грамотности среди населения; психологические особенности молодежи как возрастной группы. 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 [1].

Образовательные учреждения с целью обеспечения информационной безопасности используют большое разнообразие технических средств защиты (программные, аппаратные и программно-аппаратные комплексы): криптографические средства, обеспечивающие шифрование информации и механизмы проверки подлинности; антивирусные мониторы, фильтры, сканеры; средства, обеспечивающие отказоустойчивость и резервное копирование; межсетевые экраны и шлюзы. С каждым годом прогрессируют системы защиты от вирусных и спам атак.

Рассмотрим основные программно-аппаратные механизмы противодействия кибертерроризму.

Наиболее распространенными в образовательных учреждениях являются контент-фильтры. Контент-фильтр или программа ограничения Интернет-контента – это программное или аппаратное решение для ограничения выхода в интернет на нежелательные интернет ресурсы.

Системы контроля безопасности контента в первую очередь призваны осуществлять контроль за содержанием потоков информации, передаваемых в Интернет и получаемых из сети в локальную вычислительную сеть. К задачам систем контент-фильтрации относятся также проверка информации, хранящейся в локальной сети, контроль за содержанием электронной почты, а также контроль за просматриваемой информацией с целью предотвращения использования Интернета в личных целях [4]. Необходимость систем контент-фильтрации диктуется тем, что Интернет – это источник информации, за который никто не несет ответственности, и вероятность получения из него недостоверной, оскорбительной, пиратской или запрещенной по другим причинам информации весьма велика. Наличие во внутренней сети учебного заведения подобной информации может вызвать не только претензии к ученикам, которые подобный контент скачивают на рабочую станцию сети, но и к уголовному преследованию администрации, которая допускает хранение подобных материалов.

Отметим, что нежелательным контентом может являться также тот, который отвлекает детей от учебного процесса. Дети могут вместо выполнения учебного задания в Сети заниматься просмотром материалов разрешенного характера, но не имеющего ничего общего с учебным процессом.

Контент-фильтр помогает защитить компьютеры от вирусов, проникающих на ПК пользователей через сомнительные сайты, спам рассылок на почту. Такие фильтры работают по принципу списков сайтов, объединяемых в специальные группы в зависимости от контента (рис. 1). Процесс создания таких списков длительный во времени и трудоёмкий**,** однако он помогает устранить проблемы связанные с хищением персональных данных и ограничения доступа к контенту. Компьютер, хранящий базу с персональными данными, осуществляет подключение к Интернету через контент-фильтр путём использования защищенного SSL подключения, которое обеспечивает конфиденциальность обмена данными между клиентом и сервером, использующими TCP/IP подключение, для шифрования используется асимметричный алгоритм с открытым ключом. Таким образом, данные системы контент-фильтрации позволяет обеспечить защиту инфраструктуры как образовательных учреждений, так и корпоративный сегмент.

До сих пор мы говорили о том, что в учебном заведении есть проблема проникновения нежелательного контента внутрь учебной сети. Но существует также проблема утечки контента. В данном случае, во-первых, речь идет об утечке приватных персональных данных. В современном обществе существует проблема похищения детей, сексуальные домогательства и проч. Поэтому личная информация о ребенке (его фотография, расписание уроков, e-mail, телефон) не должны вывешиваться в Сети для свободного доступа.

При размещении фотографий в Сети (например, на школьном Web-сайте) желательно размещать фотографии детей только с согласия родителей, и только групповые. Не стоит указывать имена детей и другую личную информацию.

Вторая проблема – это рассылка по почте или размещение на школьном (или другом) сайте запрещенного контента. Рассылка пиратского ПО, порнографии и т.п.

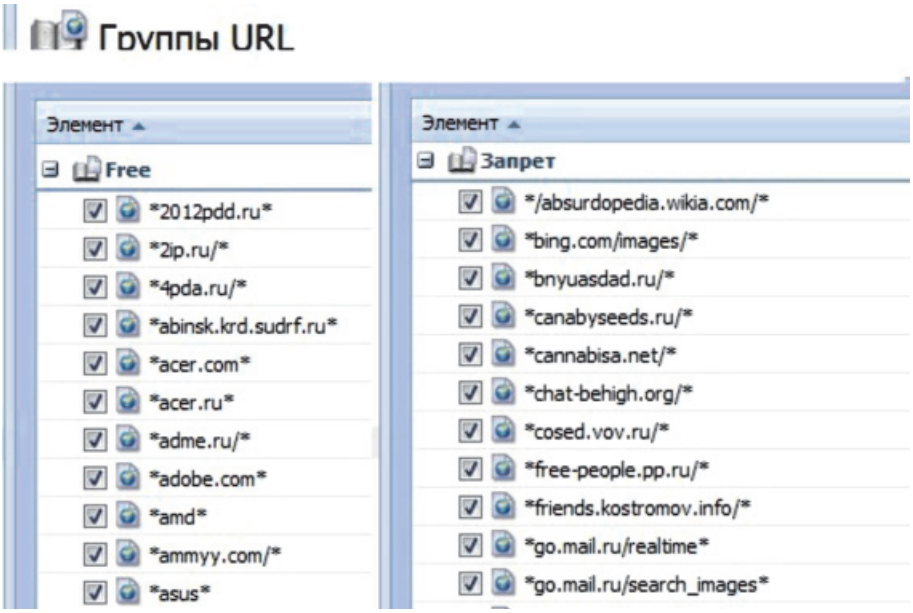

Рис. 1. Ограничение доступа по групповым спискам

Каждый день в Интернете появляются тысячи новых сайтов, поэтому, даже используя обновления баз данных с нежелательными ресурсами, добиться 100%-й фильтрации невозможно. Отдельная проблема – это недостаточная фильтрация русскоязычного контента западными продуктами. Возможны ошибки, когда фильтр будет отсеивать сайты полезного содержания. В общем, чем более интеллектуален фильтр и чем больше база, на которую он опирается, тем дороже решение и тем оно менее доступно для школ.

Администраторы в школах имеют различный опыт работы с компьютерами, и даже непрофессионал должен иметь возможность создавать и поддерживать политику фильтрации. Образовательный процесс включает множество различных областей науки, и фильтрация должна быть всеобъемлющей, настраиваемой, а также обеспечивать защиту от новейших угроз.

Другим широко используемым механизмом обеспечения информационной безопасности является мониторинг интернет-ресурсов, который дает быструю и точную картину Web серфинга (рис. 2). Данные об интернет активности защищены криптографически и хранятся в недоступном для неавторизованного просмотра виде. Любой посещенный ресурс может быть просмотрен и впоследствии добавлен в список разрешенных или запрещенных листов. Используя специальные механизмы ограничения работы по времени (рис. 3), можно задать в период учебного дня «список» порталов исключительно для образования, а во внеурочное время открыть доступ к порталам, попадающим в белый список, и не нарушая «Единый реестр» доменных имен, указателей страниц сайтов в сети Интернет [5].

Благодаря применению механизмов фильтрации и мониторинга можно не только обеспечить безопасное подключение для передачи данных, но и контролировать работу и деятельность учащихся, отслеживая посещаемость Интернет-ресурсов. Можно ограничить детей от нежелательного контента, тем самым препятствовать негативному развитию детей. Однако стоит понимать, что не все сайты будут попадать в список разрешенных, в виду разногласий в сети Интернет. Поэтому следует своевременно настраивать и редактировать список сайтов, к которым будет организован доступ, не нарушая правила «Единого реестра».

В образовательном учреждении 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 27Mindwebfilter 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.

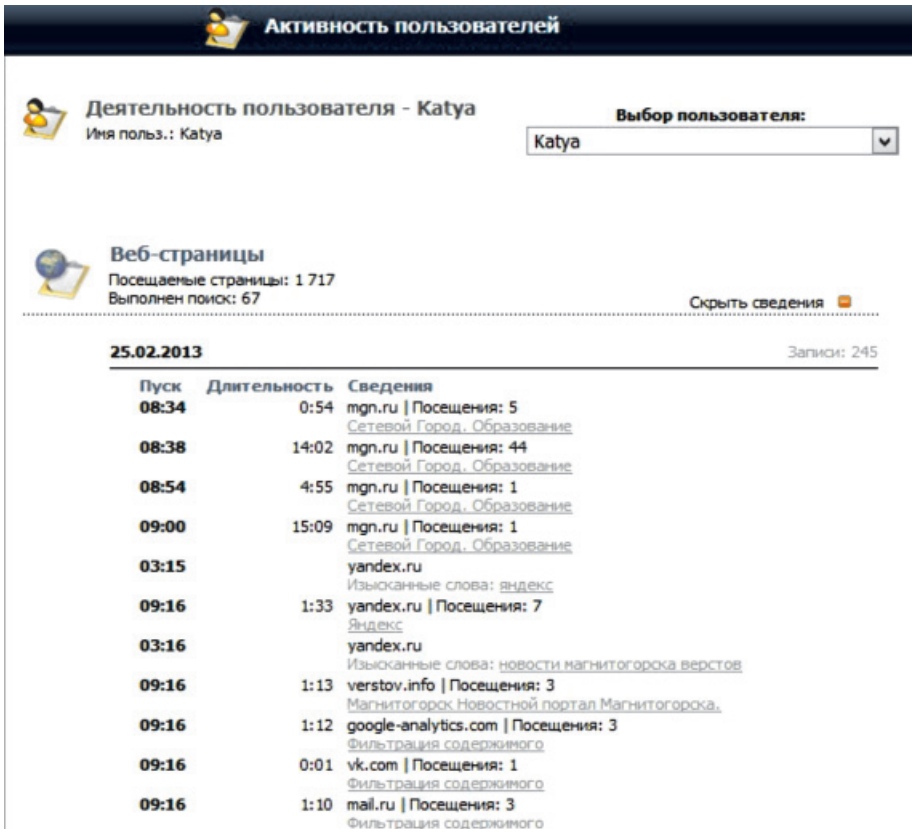

Рис. 2. Статистика посещения веб-сайтов пользователя

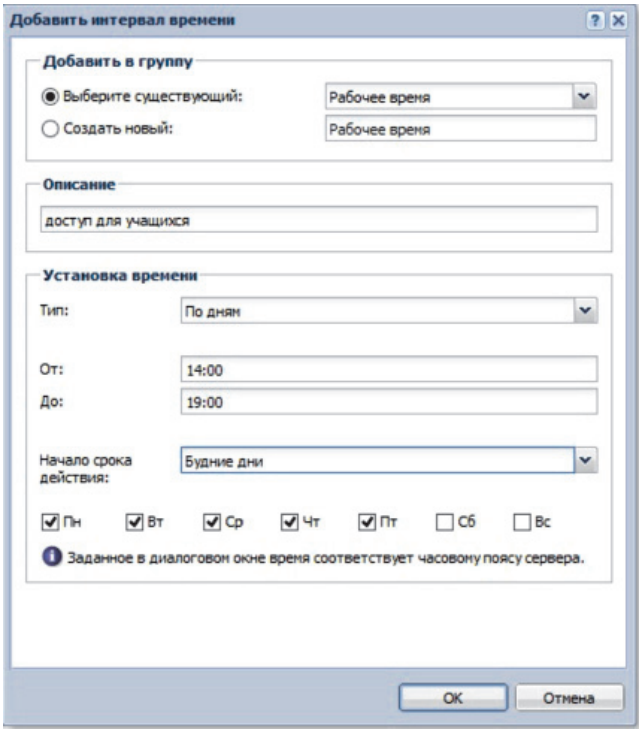

Рис. 3. Ограничение доступа по временному интервалу

С целью определения уровня компетенции в области информационной безопасности нами был проведен опрос среди учителей школ г. Магнитогорска и выявлено, что 100% знают о негативных формах и способах воздействия ИКТ; 80% знакомы с·видами отклоняющегося, зависимого от Интернет поведения школьников; 60% владеют методами работы по их предупреждению и устранению; 55% знают правила и нормы сетевого этикета; 30% (преимущественно учителя информатики) применяют методы защиты. В городе имеется опыт проведения мастер классов и педагогических советов по вопросам информационной безопасности, где выступают приглашенные специалисты вуза, консалтинговых компаний, предоставляющих услуги аудита ИБ и др. компетентных лиц.

Согласно on-line-опросу RUметрики, около половины родителей контролируют интернет-передвижения своих детей только до 10 лет. 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. Порносайты просматривают 32% интернет-аудитории детей до 14 лет. С сайтами об азартных играх, ресурсами о насилии, алкоголе и наркотиках сталкиваются от 13 до 15% школьников.

Проведя опросы среди родителей, нами выявлено, что большая часть опрошенных знакомы с блокировкой нежелательных интернет-ресурсов для посещения детьми, но не умеют пользоваться этой функцией. Таким образом, очень важно не только организовать работу по обеспечению информационной безопасности образовательного учреждения, но и повышать осведомленность учеников и родителей в этой области. Это можно делать с помощью тренингов, курсов, новостных рассылок, обучающих роликов, готовых комплексов и учебных материалов, постеров и т.д.

Таким образом, профилактика киберэкстремизма – комплексная проблема, для решения которой необходимо задействовать юридические, психолого-педагогические и технологические инструменты.

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

Список литературы

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

2. 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.

3. Крутских А.В. К политико-правовым основаниям глобальной информационной безопасности // Международные процессы. – 2007. – № 1 (13).

4. Программы контроля, родительский контроль [интернет портал]. – URL: http://nicekit.ru/parental-control/time-boss.php.

5. Gordon S. Cyberterrorism? // Symantec Security Responce. – 2010. – Mode of access.: http://www.packetsource.com/article/laws-andregulations/39683/cyberterrorism.

References

1. Abulin K.A. Besopastnost v internete [internet portal], available at: http://www.comprice.ru.

2. Zerkina E.V., Chusavitina G.N. Podgotovka buduschich uchiteley k prevencii deviantnogo povedeniya shkolnikov v cphere informacionno-kommunikacionnich technologiy: monographiya. Magnitigorsk, MaGU, 2008. 185 p.

3. Krutskich A.V. K politico-pravovim osnovaniyam globalnoy informacionnoy bezopasnosty. Mezhdunarodnie processi. 2007, no. 1 (13).

4. Programmy kontrolya, roditelskiy control [internet portal], available at: http://nicekit.ru/parental-control/time-boss.php.

5. Gordon S. Cyberterrorism? // Symantec Security Responce. 2010, available at: http://www.packetsource.com/article/laws-andregulations/39683/cyberterrorism.

Рецензенты:

Климова Т.Е., д.п.н., профессор кафедры педагогики, ФГБОУ ВПО «Магнитогорский государственный университет», г. Магнитогорск;

Овчинникова И.Г., д.п.н., профессор кафедры информатики, ФГБОУ ВПО «Магнитогорский государственный университет», г. Магнитогорск.

Работа поступила в редакцию 17.10.2013.