УДК 004.056.5
ББК 32.973-018.2

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ОБРАЗОВАНИИ: ОБУЧАЮЩИХСЯ И ОБУЧАЮЩИХ

А. Я. Минин

Аннотация. *В статье обосновывается, что правовые вопросы противодействия угрозам кибер- или информационной безопасности обучающихся и обучающих в общеобразовательной и высшей школе могут быть решены и решаются достаточно эффективно и результативно благодаря совершенствованию правового регулирования образовательной деятельности, а также применению современных методов социального контроля и надзора за исполнением российского законодательства в сфере образования, предупреждения девиаций в сети Интернет. Существенную роль играет система воспитания и социального контроля как механизм гарантии информационной культуры и неотвратимости воздействия на девиантное поведение в информационно-телекоммуникационной сети.*

Ключевые слова: *кибербезопасность в образовании, правовое регулирование, противодействие угрозам в ИТКС Интернет, сфера высшего и общего образования, значимость информационной культуры, воспитания и социального контроля.*

INFORMATION SECURITY IN EDUCATION: STUDENTS AND TEACHERS

A. Ya. Minin

Abstract. *The article elaborates on the problems of information security of education and shows that legal problems of counteraction to cyber-threats for schoolboys, students and teachers in higher educational institutions and schools may be effectively solved thanks to the improvement of legal regulation of educational activity, and also implementation of modern methods of social control and supervision over the observance of the Russian legislation in education, prevention of deviance on the Internet. A significant role is played by the education system and social control as a mechanism of guarantee of information culture and inevitability of influence on deviant behavior in telecommunications network.*

Keywords: *information security (cybersecurity) in education, legal regulation, counteraction to cyber-threats in Internet, general and higher education , importance (role) of informational culture, education and social control.*

В современной литературе существуют дискуссионные понятия кибербезопасности и ее глобальной культуры, киберпространства и безопасного поведения в нем, защиты детей от негативной или вредной информации в информационно-телекоммуникационной сети (далее – ИТКС) Интернет. Кибербезопасность – состояние защищенности киберпространства, сложной среды, создаваемой совокупностью информации, информационной среды и информационного взаимодействия людей. По стандарту ISO 27032:2012 [1], термин «кибербезопасность» связывают в основном с сетевой безопасностью (так ее интуитивно и воспринимает 83,3% опрошенных студентов 1-го курса ИСГО МПГУ, направление «Юриспруденция»), прикладной безопасностью, интернет-безопасностью и безопасностью критичных информационных инфраструктур. Комплексное состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, образовательных в том числе, общества и государства, – это информационная безопасность.

Информационная безопасность в образовании включает три составляющие: конфиденциальность – защита чувствительной информации обучающихся и обучающих от несанкционированного доступа; целостность – защита точности и полноты информации и программ-

ного обеспечения учебного процесса; доступность – обеспечение доступности информации для познавательного процесса, а также основных информационно-библиотечных и иных услуг для пользователя, несовершеннолетнего обучающегося в том числе, и в нужное для него время: в рамках учебного процесса в образовательной организации или вне ее для индивидуальной работы в домашних условиях [2, с. 117–118]. Обучающиеся уже имеют представление об основных трех составляющих кибербезопасности в образовании. Так, по результатам опроса 1-го курса ИСГО МПГУ, конфиденциальность персональных данных, деликатной или чувствительной информации указали 66,6%; целостность информации – 38,8%; доступность информации, информационно-библиотечных услуг – 16,6%; при этом 83,3% респондентов интуитивно, но ошибочно выделили также и киберустойчивость, киберзащиту.

Правовое обеспечение информационной безопасности в образовательной организации. Разработаны Концепция информационной безопасности детей, Национальная стратегия действий в интересах детей на 2012–2017 гг., одно из основных направлений реализации которой – обеспечение информационной безопасности детей [3]; Закон 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» и др. [4]. Так, Закон №149-ФЗ «Об информации...» содержит ст. 12, в которой п. 1 гласит: Госрегулирование в сфере применения ИТ предусматривает: <…> 4) обеспечение информационной безопасности детей (п. 4 введен 21.07.2011 № 252-ФЗ); ст. 15.1. Единый реестр доменных имен, указателей страниц сайтов в ИТКС и сетевых адресов, позволяющих идентифицировать сайты в ИТКС, содержащие информацию, распространение которой в РФ запрещено, – в п. 5 к основаниям для включения в реестр сведений отнесены: 1) решения уполномоченных Правительством РФ федеральных органов исполнительной власти, принятые в соответствии с их компетенцией в установленном порядке в отношении распространяемых посредством ИТКС: а) материалов с порнографическими изображениями несовершеннолетних и/или объявлений о привлечении их в качестве исполнителей для участия в зрелищных мероприятиях порнохарактера; <…> г) информация о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), распространение которых запрещено федеральными законами (пп. «г» введен 05.04.2013 № 50-ФЗ).

Следственный комитет Российской Федерации (далее – СК РФ) беспокоит легкомысленное отношение к ограничениям и запретам, установленным Законом 436-ФЗ, что зачастую не позволяет просчитать последствия от их нарушения, приобретающие в некоторых случаях характер общественно опасных. Только в 2014 г. по сравнению с 2013 г. на 70% возросло количество маленьких самоубийц, из жизни добровольно ушло 784 ребенка. Сколько бы ни запрещали, но и сейчас подросток может прочесть про клуб самоубийц и прочую вредную информацию, которую не стоит знать детям. Отсюда и детские самоубийства, и детская агрессия. В связи с этим предлагается установить уголовную ответственность за незаконный оборот инфопродукции, если она содержит информацию, побуждающую детей к совершению насильственных действий или самоубийству. Коснулся СК РФ и такой темы, как сроки давности привлечения к уголовной ответственности за преступления, совершенные в отношении половой неприкосновенности детей. Ребенок, против которого совершено половое преступление, может заговорить о нем не сразу просто потому, что может не понимать, что с ним произошло, или стыдиться этого. Иногда проходят годы, прежде чем выявляется факт сексуального насилия; ситуация характерна для преступлений, совершаемых внутри семьи.

Позиция СК РФ: обеспечить реализацию обязательств России, предусмотренных ратифицированной Конвенцией СЕ о защите детей от сексуальной эксплуатации и сексуальных злоупотреблений (2007). Важно, чтобы срок давности для привлечения к уголовной ответственности лица, совершившего преступление против половой неприкосновенности ребенка, был достаточным для эффективного возбуждения разбирательств после достижения жертвой совершеннолетия и был соразмерным тяжести преступления. Изменения, которые вносятся в ст. 78 УК РФ, предусматривают, что сроки давности для таких преступлений начинают исчисляться со дня достижения жертвой восемнадцатилетнего возраста.

Угрозы кибербезопасности в ИТКС Интернет и технологии противодействия им. Доля интернет-пользователей в Евросоюзе, которые столкнулись с проблемами в области информационной безопасности в 2015 г., составляет порядка 25%, сообщает RNS со ссылкой на статистическую службу Евростата. Каждый четвертый житель Евросоюза столкнулся с такими проблемами, как поражение устройств вирусами, доступ к нежелательным сайтам детьми, злоупотребление при использовании персональной информации о пользователях, финансовые потери[1]. Молодые люди склонны думать, что они опытнее в использовании новых технологий, по сравнению со старшим поколением. Вместе с тем за последний год порядка 13% их представителей от 18 до 24 лет по всему миру потеряли деньги в интернет- и телефонных мошенничествах, и 20% тех, кому от 25 до 34 лет. При этом среди людей старше 65 лет эта цифра составляет всего 3%. За последний год звонки от преступников получали 23% молодых лиц от 18 до 24 лет и 29% опрошенных от 25 до 34 лет. В то же время с переадресацией на сомнительный интернет-ресурс сталкивались 50% и 49% среди этих возрастных групп соответственно[2].

В рамках проводимой МВД России международной операции «Сорняк» в разных странах мира выявлено 1803 пользователя пиринговых (англ. peer-to-peer, P2P – «равный к равному») сетей, распространяющих видеоматериалы, содержащие «детскую» порнографию; из них 232 потребителя из 47 регионов РФ. Возбуждено 169 уголовных дел по выявленным фактам. В правоохранительные органы 63 иностранных государств направлена информация (всего 304 материала) о противозаконной деятельности их граждан. Так, примерный перечень угроз в ИТКС Интернет составляет порядка 14 категорий доступных сайтов с нежелательными ресурсами в РФ: порно, эротика (46,4%), социальные сети (27,5%), оружие (26,4%), ненормативная лексика (10,7%), нелегальное ПО (6,6%), онлайн-игры (5,5%), азартные игры (1,9%), жестокость и насилие (1,1%), анонимные прокси-серверы (0,7%), платежные системы (0,4%), наркотики (0,3%), онлайн-магазины, чаты, электронная почта (0,2%). В скобках здесь указано распределение процента посещаемости нежелательных сайтов этих категорий (Россия, январь–май 2014)[3].

Кибертеррор (cyberbully). Во многих странах дети и в особенности подростки часто сталкиваются в ИТКС с кибербуллингом – травлей жертвы через Интернет. Агрессоры действуют через все возможные каналы общения: социальные сети, форумы, чаты, мессенджеры, причиняя жертве серьезные душевные страдания, которые могут привести к психологической травме и/или к суициду. Осуществлять травлю могут как знакомые жертвы (одноклассники, соседи, интернет-друзья и т. д.), так и совершенно посторонние люди. Так, увидев фотографию жертвы в ИТКС и пользуясь относительной анонимностью Интернета, агрессоры ради развлечения могут затравить ребенка, привлекая к участию в травле себе подобных в интернет-сообществах. Формы травли: нанесение оскорблений через личные сообщения, публикация провокационных материалов, распространение конфиденциальной информации о жертве. Цели: подростковое баловство, получение выгоды, доведение жертвы до самоубийства. Борьба с кибертравлей технически не так проста, поэтому и программный «Родительский контроль» не столь эффективен. При этом дети не способны справиться с агрессорами в одиночку, но зачастую не обращаются к взрослым за помощью, будучи запуганными угрозами, либо просто из-за отсутствия доверия к близким людям. Отношения с родителями и педагогами играют важную роль в защите ребенка от кибербуллинга.

Особенности воспитания и подготовки обучающихся к информационным угрозам. Известная формула безопасности: Безопасность ребенка в ИТКС = Контроль со стороны родителей + «Родительский контроль». Функция «Родительский контроль» продукта KIS («Лаборатория Касперского») – инструмент,

[1] http://d-russia.ru/chetvert-evropejskix-internet-polzovatelej-stolknulis-s-problemami-bezopasnosti-v-2015-godu-issledovanie.html

[2] https://news.microsoft.com/ru-ru/features/molodezh-chashhe-drugih-stanovitsya-zhertvoj-kibermoshennikov/#sm.0001bd0oge9aveeosf41x9jx37yf6#p5LHXDqFF9GMEH4D.97

[3] https://securelist.ru/analysis/obzor/20171/deti-v-seti-formula-bezopasnosti/

обеспечивающий защиту от нежелательной и опасной для ребенка информации в ИТКС Интернет. Но полагаться только на программное обеспечение не стоит. Педагоги и родители должны помнить об ответственности за безопасность ребенка, не перекладывая ее полностью на программные и технические средства защиты. Важную роль играет воспитание, подготовка ребенка к информационным угрозам, ведь он никуда не денется от необходимости активного использования информационно-телекоммуникационных сетей. Так, российские дети получают первый мобильный телефон в 7–8 лет (в США, Германии Великобритании – ближе к 10 годам). И когда они проявляют самостоятельность, важно использовать программный продукт для родительского контроля. Например, мобильное приложение ESET NOD32 Parental Control для Android не только защитит от онлайн-рисков, но и позволит отследить местоположение ребенка в онлайн-режиме, оперативно связаться с ним, отправив сообщение «Позвони домой!», которое автоматически выводится на экран. По данным опроса ESET, такой контроль в России использует порядка 56% родителей.

В Евросоюзе действует возрастной лимит 16+ на использование социальных сетей[4]. Европарламент принял закон о защите данных General Data Protection Regulation, который с 2017 г. запретит подросткам 13–16 лет регистрироваться в социальных сетях. Обрабатывать персональные данные подростка до 13–16 лет возможно только с родительского согласия, иначе доступ тинейджеров эффективно блокируется в социальной сети и к другим сервисам, которые обрабатывают персональные данные или именную информацию. Чтобы зарегистрироваться в Facebook (Instagram, WhatsApp), подростку потребуется предоставить явное согласие родителя или опекуна. Для IT-компаний проблема в том, что новый закон технически сложно соблюдать. Неясно, как проверять наличие родительского контроля при использовании сервиса и реализовать процедуру получения родительского согласия.

Современные меры и средства защиты их от вредной и нежелательной информации в образовательной организации и вне ее в домашних условиях. Рассмотрим известные программы для обеспечения безопасности детей, включая антивирусы с нужной функцией. Так, браузер «Спутник» для ОС Windows имеет таймер «Детский режим», который позволяет родителям установить ребенку ограничение на доступ в Интернет. Защиту детей от порно в ИТКС обеспечивают и специальные программы для запрета порнографии, и антивирусные пакеты. Конечно, у них нет опций вроде запрета доступа к секс-чатам или «блокировка защиты паролем», однако оградить детей от нежелательного контента в ИТКС они вполне способны. Продукт «Лаборатории Касперского» – Kaspersky Internet Security – обладает функцией «Родительский контроль». Благодаря этому компоненту для каждой учетной записи на ПК возможно установить ограничения. Например, открыть закладку «Посещение веб-сайтов» и указать страницы, на который вход будет запрещен, поставить галочку напротив категории «Порно, эротика», заблокировав тем самым доступ к сайтам с таким содержимым. Подобную услугу предлагает и продукт «Доктор Веб». Его «Модуль родительского контроля» не только ограничивает доступ к сайтам, где показаны «взрослые игры», но и вычисляет ресурсы локальной сети и папки на ПК, в названии или описании которых есть слова, связанные с индустрией развлечений для взрослых. Для того чтобы активировать защиту от порнографии в ИТКС, необходимо зайти в «Настройки» – «Фильтры URL» и поставить галочку напротив категории «Сайты для взрослых».

Ясно, что не все россияне использует функцию «Родительский контроль». Вместе с тем 14% из них потеряли деньги или важную информацию в результате действий своих детей в ИТКС, выяснили специалисты B2B International, опросив для «Лаборатории Касперского» 11 135 респондентов старше 16 лет, проживающих в странах Латинской и Северной Америки, Ближнего Востока, Азии, Африки, Европы и России. При этом 43% опрошенных российских родителей уверены, что их ребенок недостаточно хорошо разбирается в компьютерных технологиях, а 45% считают, что их дети ничего не зна-

[4] http://news.softodrom.ru/ap/b24540.shtml; http://ria.ru/world/20160422/1416901114.html

ют о киберугрозах. Отсюда и риски для родителей, которые разрешают детям пользоваться своими устройствами. Так, 12% респондентов сообщили, что их дети случайно удаляли важную информацию с их компьютеров, 2% получили счета из магазинов приложений; 20% опрошенных родителей рассказали, что за последний год с их детьми случались инциденты, угрожавшие непосредственно детям. Для снижения потерь и защиты детей от интернет-угроз 36% родителей ограничивают время, проводимое детьми в ИТКС, но журнал браузера проверяют 24%; 26% регулярно разговаривают с детьми о киберугрозах, и 14% добавились к ним в друзья в социальных сетях. В то же время специализированное программное обеспечение для контроля действий детей в ИТКС применяют лишь 19% опрошенных родителей. Когда речь идет о детях в ИТКС Интернет, важно защитить их от нежелательного контента в Сети. Использование родительского контроля – не проявление недоверия к ребенку, но разумная мера предосторожности, позволяющая защитить и данные, и само устройство. Не стоит выпускать из вида и угрозу для их родителей. По мнению руководителя группы анализа веб-контента «Лаборатории Касперского», взрослые дети могут применить такие программные продукты и в отношении своих мало осведомленных о киберугрозах родителей[5].

Осуществление полноценного контроля содержимого сайтов, которые может открыть ребенок, можно доверить и утилите Anti-Porn, которая способна автоматически скрывать запрещенные сайты и неприличные баннеры, блокировать не только эротический и порноконтент, но также чаты и различные игры. Программа запрета порносайтов работает с онлайн- и офлайн-контентом. Таким образом, родители могут ограничить время, проводимое ребенком в ИТКС. Anti-Porn хранит информацию обо всех посещаемых сайтах и может предоставить данные о статусе их просмотра.

Blue Coat K9 Web Protection позволяет ограничить доступ к нежелательным ресурсам. Работает по принципу антивируса, имеет объединенную базу от всех пользователей на определенном сервере. Сразу же после установки программа готова бороться с запрещенными сайтами. Как только вводится адрес интернет-ресурса, отправляется запрос к внешней базе данных. Сайты базы разбиты по категориям: ресурсы для взрослых; содержащие элементы насилия; рекламирующие сигареты, оружие и алкоголь; рассылающие фишинг- и вредоносные программы. При установке программы можно активировать функцию безопасного поиска, а в специальной вкладке указать сайты, которые должны блокироваться всегда. Для любителей сидеть в ИТКС сутки напролет можно ограничить время нахождения в сети. Программа позволяет просматривать журнал web-активности за определенный период. То есть можно получить информацию о сайтах, которые запрашивались, их количестве и статусе просмотра. Несмотря на функциональность, программа для блокирования порносайтов имеет недочеты: приложение не русифицировано, требуется регистрация.

BitTally создана для учета и контроля интернет-трафика (бесплатная полная версия). Кроме того, пользователю предоставляется возможность отслеживать посещение web-страниц с подозрительным или нежелательным контентом и устанавливать на них блокировку. Используя функцию «Родительский контроль», можно установить запрет на посещение сайтов с нецензурной лексикой и пропагандой наркотиков и насилия, порносайтов, сайтов для онлайн-знакомств. Таким образом мы ограждаем детей от доступа к сайтам, способным нанести вред их неукрепившейся психике (вызвать страх, панику, внушить ужас), пока взрослых не будет дома. Кроме того, можно установить фильтры и права доступа к ИТКС в случае, если ПК будут пользоваться дети или гости. Алгоритм, по которому работает данный софт, следующий: в базе ПО, где более 50 тыс. URL определенных категорий, разыскивается адрес. Если он не обнаружен, поиск ведется по доступному для редактирования списку категорий. Если его и там нет, BitTally проанализирует контекст сайта и выделит его теги. Так она определит, насколько опасной для детей может быть данная страница. Недостаток программы – нагрузка на процессор и переизбыток различных отчетов.

[5] http://www.astera.ru/news/?id=108045; http://www.entensys.com/ru/products/kindergate-parental-control/overview

Используемые в российских школах интернет-фильтры приведены в соответствие с рекомендациями Минобрнауки России [5]. «Методические рекомендации по ограничению в ОО доступа обучающихся к видам информации, распространяемой посредством ИТКС Интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования» были приняты Минобрнауки еще в 2014 г. и согласованы с Минкомсвязи России и Временной комиссией Совета Федерации по развитию информационного общества. Так, издание CNews сообщило, что компания Entensys привела свои продукты UserGate Web Filter и «KinderGate Родительский Контроль», используемые для интернет-фильтрации, в соответствие с установленными требованиями. Вышеупомянутые решения используются в образовательных организациях (в российских школах свыше 12 тыс.). Наш опрос обучающихся показал, что 77,7% первокурсников знают о применении в российских школах ПО для интернет-фильтрации нежелательного контента в ИТКС; 33% из них известно об использовании родителями знакомых ребят программных продуктов с функцией "Parental Control". Основные источники их знаний об угрозах – это уроки по кибербезопасности в старших классах (указали 72,2%), продвинутые пользователи из ближайшего окружения (50%), собственный опыт (11,1%), форумы в ИТКС Интернет (5,5%). Лишь 5,6% обучающихся и обучающих используют программы для хранения паролей, например бесплатный менеджер паролей Keepass.

В Entensys уверены, что продукты компании должны соответствовать рекомендациям Минобрнауки, в связи с чем были реализованы некоторые изменения в интернет-фильтрах. В частности, в UserGate Web Filter и «KinderGate Родительский Контроль» стандартные настройки фильтрации приведены в соответствие с «Перечнем видов информации, распространяемой посредством сети Интернет, причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования». Возможность работы с Реестром несовместимых с образованием ресурсов ожидается в ближайшем будущем. Также в фильтрах реализованы все возможные способы подключения системы контентной фильтрации, указанные в рекомендациях Минобрнауки России.

Согласно Концепции информационной безопасности детей [3], важно продолжать работу по совершенствованию механизма блокировки сайтов в ИТКС, содержащих запрещенную информацию. В настоящее время доказала свою эффективность существующая система включения пяти видов особо опасной социальной информации, доступ к которой безусловно должен быть запрещен, в Единый реестр доменных имен, указателей страниц сайтов в ИТКС и сетевых адресов, позволяющих идентифицировать сайты в ИТКС Интернет, содержащие информацию, распространение которой в Российской Федерации запрещено. К таким видам информации относят детскую порнографию, информацию о продаже наркотиков, призывы к осуществлению самоубийств, информацию о пострадавшем в результате противоправных действий (бездействия) несовершеннолетнем, информацию, нарушающую требования Законов «О госрегулировании деятельности по организации и проведению азартных игр…» и «О лотереях», о запрете деятельности по организации и проведению азартных игр и лотерей с использованием ИТКС, средств связи.

В процессе воспитания обучающихся и овладения ими необходимым уровнем информационной культуры важно не упустить из виду крайне малую вероятность их десоциализации: выбора ими модели отклоняющегося поведения так называемых «теневых хакеров», ориентированных на криминальный промысел и опасные деяния в сфере компьютерной информации. Молодежь – костяк групп киберпреступников, заметно растущей прослойки компьютерных мошенников, работающих в строго иерархических структурах и нуждающихся в низовом звене исполнителей (например, дропперы, снимающие деньги с банковской карты).

Так, компания HackerOne представила отчет "Bug Bounty Report 2016" о ходе исследования: опрос 617 специалистов из базы данных, в которой зарегистрированы свыше 70 тысяч «легальных хакеров» (то есть лиц, ищущих уязвимости за вознаграждение в рамках официаль-

ных программ) из 70 стран мира[6]. Согласно исследованию, большинство из них живут в Индии (21%), США (19%) и России (8%); 90% хакеров моложе 34 лет (в том числе 43,5% – от 18 до 24 лет, 41,4% – 25–34 года); 25,9% – студенты; 39% – работают в компаниях, занимающихся компьютерной безопасностью. 71,5% опрошенных заявили, что занимаются этим ради денег, 70,5% – «ради забавы», 65,9% – чтобы испытать себя, 64,3% – ради резюме, а 50,8% – хотят «сделать мир лучше».

Таким образом, одна из актуальных задач воспитания обучающихся состоит в подготовке их к грамотному использованию компьютерных и сетевых технологий, например, в профессиональной педагогической или юридической деятельности, в учебном процессе образовательной организации и вне ее стен, в домашних условиях и в общественных местах с доступом к информационно-телекоммуникационным сетям. Кроме того, все обучающие должны уметь обогатить знания, умения и навыки обучающихся новыми аспектами безопасной работы в ИТКС Интернет, передать необходимые ИКТ-компетенции учителей (принципы, модули, реализация) студентам педагогических вузов. Поэтому сегодня и возникает еще большая потребность в том, чтобы обучающий обладал практическими навыками (новая роль педагога, учителя), зависящими от уровня его познаний, информационной культуры использования ИКТ, определенными ЮНЕСКО [6] и Международным обществом по информационным технологиям в образовании (ISTE).

СПИСОК ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. Международный стандарт ИСО/МЭК 27032: 2012 Руководящие указания по кибербезопасности «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по кибербезопасности» (ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity).
2. *Минин А. Я.* Информационные технологии в образовании: учеб. пособие. – М.: МПГУ, 2016. – 148 с.
3. Концепция информационной безопасности детей, утв. распоряжением Правительства РФ от 02.12.2015 №2471-р. Национальная стратегия действий в интересах детей на 2012–2017 гг., утв. Указом Президента России от 01.06.2012 № 761.
4. О защите детей от информации, причиняющей вред их здоровью и развитию. Закон от 29.12.2010 № 436-ФЗ (ред. от 29.06.2015 № 179-ФЗ). О внесении изменений в отдельные законодательные акты РФ в связи с принятием Закона № 436-ФЗ (от 26.07.2011 № 252-ФЗ). Об информации, информационных технологиях и о защите информации. Закон № 149-ФЗ от 27.07.2006 (ред. от 06.07.2016 № 374-ФЗ).
5. О направлении методических материалов для обеспечения информационной безопасности детей при использовании ресурсов сети Интернет. Письмо Минобрнауки РФ № ДЛ-115/03 от 28.04.2014 г.
6. Руководство по оценке ИКТ в образовании / Институт статистики Юнеско. – Монреаль, 2011. – 139 с. – URL: http://www.uis.unesco.org/Library/Documents/ICT_Guide_RU_final_web2.pdf (дата обращения: 14.12.2016).

REFERENCES

1. Mezhdunarodnyy standart ISO/MEK 27032: 2012 Rukovodyashchie ukazaniya po kiberbezopasnosti “Informatsionnye tekhnologii. Metody obespecheniya bezopasnosti. Rukovodyashchie ukazaniya po kiberbezopasnosti” (ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity).
2. Minin A. Ya. *Informatsionnye tekhnologii v obrazovanii: ucheb. posobie.* Moscow: MPGU, 2016. 148 p.
3. Kontseptsiya informatsionnoy bezopasnosti detey, utv. rasporyazheniem Pravitelstva RF ot 02.12.2015 No.2471-r. Natsionalnaya strategiya deystviy v interesakh detey na 2012–2017 gg., utv. Ukazom Prezidenta Rossii ot 01.06.2012 No. 761.
4. O zashchite detey ot informatsii, prichinyayushchey vred ikh zdorovyu i razvitiyu. Zakon ot 29.12.2010 No. 436-FZ (red. ot 29.06.2015 No.

[6] www.kommersant.ru/doc/3090065

179-FZ). O vnesenii izmeneniy v otdelnye zakonodatelnye akty RF v svyazi s prinyatiem Zakona No. 436-FZ (ot 26.07.2011 No. 252-FZ). Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii. Zakon No. 149-FZ ot 27.07.2006 (red. ot 06.07.2016 No. 374-FZ).

5. O napravlenii metodicheskikh materialov dlya obespecheniya informatsionnoy bezopasnosti detey pri ispolzovanii resursov seti Internet. Pismo Minobrnauki RF No. DL-115/03 ot 28.04.2014.
6. Rukovodstvo po otsenke IKT v obrazovanii / Institut statistiki Yunesko. Monreal, 2011. 139 p. *Available at:* http://www.uis.unesco.org/Library/Documents/ICT_Guide_RU_final_web2.pdf (accessed: 14.12.2016).

Минин Анатолий Яковлевич, доктор юридических наук, профессор; и. о. заведующего кафедрой уголовно-правовых дисциплин Института социально-гуманитарного образования Московского педагогического государственного университета; действительный член Международной академии наук педагогического образования (МАНПО)

e-mail: aya.minin@mpgu.edu

Minin Anatolii Ya., ScD in Jurisprudence, Professor, Acting Chairperson, Criminal Law Disciplines Department, Institute of socio-humanitarian education, Moscow State University of Education, Full Member, International Teacher's Training Academy of Science

e-mail: aya.minin@mpgu.edu