ЗАКОН О ЗАЩИТЕ ДЕТЕЙ ОТ ИНФОРМАЦИИ, ПРИЧИНЯЮЩЕЙ ВРЕД ИХ ЗДОРОВЬЮ И РАЗВИТИЮ

На этом занятии рассматривается Федеральный закон, посвященный защите детей от вредной информации и даются принципы организации защиты детей.

О законе

В России 1 сентября 2012 года вступил в силу Федеральный закон от 29.12.2010 N 436-ФЗ (ред. от 28.07.2012) "О защите детей от информации, причиняющей вред их здоровью и развитию".

Данный закон регулирует отношения, связанные с защитой детей от травмирующего их психику информационного воздействия, жестокости и насилия в общедоступных СМИ. К информации, запрещенной для оборота среди детей, относится информация:

- побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству;
- способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;
- обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным, за исключением случаев, предусмотренных настоящим Федеральным законом;
- отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;
- оправдывающая противоправное поведение;
- содержащая нецензурную брань;
- содержащая информацию порнографического характера.

Оборот такой информации не допускается среди детей в местах, доступных для детей, без применения административных и организационных мер, технических, программно-аппаратных средств защиты детей от такой информации.

В Законе сформулировано понятие **информационная безопасность детей** - состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию.

Детей и подростков, без всякого сомнения, нужно защищать от разрушающего информационного воздействия на их несформировавшуюся личность. Кроме этого, информационная продукция, запрещенная для детей, не может распространяться в предназначенных для детей образовательных организациях, детских медицинских, санаторно-курортных, физкультурно-спортивных организациях, организациях культуры, организациях отдыха и оздоровления детей или на расстоянии менее чем сто метров от границ территории этих организаций.

В Законе определяются виды информации, распространение которой среди детей определенных возрастных категорий ограничено, к ней относится информация:

- представляемая в виде изображения или описания жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия;
- вызывающая у детей страх, ужас или панику, в том числе представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий;
- представляемая в виде изображения или описания половых отношений между мужчиной и женщиной;
- содержащая бранные слова и выражения, не относящиеся к нецензурной брани.

Распространение такой информационной продукции допускается среди детей определенных возрастных групп при соблюдении обладателем информации установленного законом порядка доступа детей к информации (в частности, при условии, что в информационной продукции содержится идея торжества добра над злом, сострадание к жертве насилия, осуждение насилия, а изображение и описание насилия,

жестокости, антиобщественных действий носит ненатуралистический, кратковременный или эпизодический характер и т.п.).

Законом устанавливается классификация информационной продукции по пяти возрастным категориям:

1. информационная продукция для детей, не достигших возраста шести лет;
2. информационная продукция для детей, достигших возраста шести лет;
3. информационная продукция для детей, достигших возраста двенадцати лет;
4. информационная продукция для детей, достигших возраста шестнадцати лет;
5. информационная продукция, запрещенная для детей.

Информационная продукция для детей - информационная продукция, соответствующая по тематике, содержанию и художественному оформлению физическому, психическому, духовному и нравственному развитию детей;

Для того чтобы указанный Закон мог реализовываться, ряд федеральных законов были адаптированы к положениям 436-ФЗ. Было установлено, что с 1 сентября 2012 года будет запрещено использовать в школах и других образовательных учреждениях учебники и пособия, содержащие вредную информацию. На юридических и физических лиц с той же даты возложена обязанность обеспечивать информационную безопасность несовершеннолетних.

За нарушение законодательства в этой сфере предусмотрена административная ответственность: для граждан - штраф от 2 тыс. до 3 тыс. рублей, для должностных лиц - от 5 тыс. до 10 тыс. рублей, для предпринимателей - от 5 тыс. до 10 тыс. рублей и административное приостановление деятельности до 90 суток, для юридических лиц - штраф от 20 тыс. до 50 тыс. рублей и административное приостановление деятельности до 90 суток.

В Законе также предусмотрена ответственность за размещение в сети Интернет информации для детей, причиняющей вред их здоровью и развитию, в частности штрафы: для граждан - от 1 тыс. до 1 тыс. 500 рублей; для должностных лиц - от 2 тыс. до 3 тыс. рублей; для юридических лиц - от 20 тыс. до 30 тыс. рублей.

28 июля 2012 года был принят Федеральный закон № 139-ФЗ, изменяющий и дополняющий Федеральный закон 436-ФЗ. Изменения направлены на уточнение множества изменений в 436-ФЗ, а самое главное, регламентируют способы маркировки контента. Создан механизм принудительного блокирования интернет-страниц, содержащих информацию, запрещенную для распространения на территории Российской Федерации хостинг-провайдерами, операторами связи. И что очень важно, вводится обязанность владельцев интернет-сайтов удалить интернет-страницу, на которой размещается запрещенная к распространению информация, после получения соответствующего уведомления от хостинг-провайдера.

В 2012 году создана Единая автоматизированная информационная система "Единый реестр доменных имен и (или) универсальных указателей страниц сайтов в сети Интернет и сетевых адресов сайтов в сети Интернет, содержащих информацию, запрещенную к распространению на территории Российской Федерации" (далее - Реестр), в который с 01.11.12 включены сайты сети Интернет, на которых распространяется запрещенная информация.

Главная цель создания такого реестра - ограничение доступа к сайтам, на которых размещается информация, запрещенная для распространения. При обнаружении неправомерного контента любой пользователь может зайти на сайт http://eais.rkn.gov.ru сообщить о незаконной информации. Для приема обращений создана специальная электронная форма. Сам реестр ведет Федеральная служба по надзору в сфере связи, ИТ и массовых коммуникаций (Роскомнадзор).

За период с 26 июля по 1 августа 2013 года Роскомнадзор получил 1499 обращений с данными о сайтах с противоправным контентом. По итогам рассмотрения обращений в Единый реестр внесено 167 новых записей. В настоящее время в Реестре содержится 2604 записи, в которых из общего количества в 2220 случаях (85%) дается указание на сайты, пропагандирующие наркоманию, 289 (11%) - суицид, 95 (3,6%) - на ресурсы с детской порнографией.

Общие принципы организации защиты детей от вредной информации

Защита детей от вредной информации основывается на понятии **информационной безопасности личности** - состоянии защищенности личности, обеспечивающей ее целостность как активного социального субъекта и возможностей развития в условиях информационного взаимодействия с окружающей средой.

Информационная безопасность личности - это состояние человека, в котором его личности не может быть нанесен существенный ущерб путем оказания воздействия на окружающее информационное пространство. Жизненно важные интересы личности в информационной сфере следующие.

1. Соблюдение и реализация конституционных прав на поиск, получение прав и распространение информации.
2. Реализация прав гражданина на неприкосновенность частной жизни.
3. Использование информации в интересах деятельности, направленной на физическое, духовное, интеллектуальное развитие.
4. Защита прав на объекты интеллектуальной собственности.
5. Обеспечение прав гражданина на защиту своего здоровья от неосознаваемой вредной информации.

Особое место среди объектов защиты в системе обеспечения информационной безопасности занимает защита от воздействия **"вредной" (вредоносной) информации**.

К "вредной" информации относят:

- информацию, возбуждающую социальную, расовую, национальную или религиозную ненависть и вражду;
- призывы к войне;
- пропаганду ненависти, вражды и превосходства;
- распространение порнографии;
- посягательство на честь, доброе имя и деловую репутацию людей;
- рекламу (недобросовестную, недостоверную, неэтичную, заведомо ложную, скрытую);
- информацию, оказывающую деструктивное воздействие на психику людей, неосознаваемое ими.

Принципы организации защиты детей от вредной информации

Сформулируем основные принципы организации защиты детей от вредной информации. Под принципами защиты информации (ЗИ) понимаются основные идеи и важнейшие рекомендации по вопросам организации и осуществления работ для эффективной защиты детей от вредоносной информации.

1. **Принцип объединения усилий всех заинтересованных сторон при доминирующей позиции государства**. Указанный принцип основывается на общности целей всех субъектов обеспечения информационной безопасности личности ребенка (государство, социальные институты, общественные организации, родители, педагогическое сообщество). Общность целей создает необходимые предпосылки для объединения усилий и выработки совместных действий в интересах детей. При этом государству отводится главенствующая роль, определяемая его возможностями и ресурсами.
2. **Принцип непрерывности, последовательности и комплексности**. Этот принцип проистекает из того, что ребенок оказывается окружен информационными потоками в течение всей своей жизни, и недопустимо полагать, что только в школе, например, необходимо заботиться об ограждении детей от опасного контента. Принцип предполагает формирование исчерпывающего комплекса мер по защите ребенка от вредной информации и последовательную, с учетом возрастных и психологических особенностей ребенка реализацию его во всех точках информационного пространства личности ребенка. Для защиты детей от вредной информации во всем многообразии структурных элементов должны применяться все виды и формы защиты в полном объеме. Недопустимо применять лишь отдельные формы или технические средства. Комплексный характер защиты проистекает из того, что защита - это специфическое явление, представляющее собой сложную систему неразрывно взаимосвязанных и взаимозависимых процессов, каждый из которых в свою очередь имеет множество различных взаимообусловливающих друг друга сторон, свойств, тенденций.
3. **Принцип построения системы защиты от вредоносной информации** на основе научно-методического обеспечения. Для того чтобы организовать эффективную защиту от вредоносного информационного окружения, необходимо разработать и в дальнейшем опираться на принятую и одобренную научным сообществом концепцию обеспечения информационной безопасности личности ребенка. Такого рода концепция должна включать: систему современных взглядов, идей, целевых установок и приоритетных направлений, общие положения, принципы, содержание, технологию, методологические и теоретические положения профессиональной деятельности субъектов процесса обеспечения информационной безопасности личности ребенка.
4. **Принцип открытости** предполагает широкое информационное сопровождение деятельности по обеспечению информационной безопасности личности ребенка, создание информационных ресурсов, где освещались бы описания угроз личности ребенка и методических рекомендаций для родителей, учителей, работников специальных служб по проведению профилактической деятельности.

5. **Принцип возможности создания для ребенка инфобезопасной среды дома и в школе**. В соответствии с этим принципом необходимо создать информационно-образовательную среду, дополнить ее аппаратными, программными и организационными средствами и способами защиты от негативной информации. Такая инфобезопасная среда должна обеспечивать безопасность и защиту личностной информационной среды ребенка в целях создания условий для его наиболее полноценного развития и реализации индивидуальных способностей и возможностей.
6. **Принцип роста защищенности жизни человека будущего**: рост знаний человека, совершенствование техники и технологии, применение мер защиты, ослабление социальной напряженности - в будущем неизбежно приведут к повышению защищенности человека от опасностей. Этот принцип сформулирован, опираясь на принцип Ле Шателье: "Эволюция любой системы идет в направлении снижения потенциальной опасности".

На основании принципов можно выделить **уровни защиты детей от вредной информации**:

1. **Концептуально-политический**. На этом уровне принимаются документы, в которых определяются основные направления государственной политики в области информационной безопасности, формулируются цели и задачи обеспечения информационной безопасности в отношении всех обозначенных субъектов, намечаются пути и средства реализации поставленных целей. Примером подобного рода документов является Доктрина информационной безопасности РФ, утвержденная Президентом РФ 9 сентября 2000 г. и Стратегия национальной безопасности Российской Федерации до 2020 года.
2. **Законодательный**. На этом уровне принимаются нормативные правовые акты (законы, постановления правительства и др.), призванные инициировать создание и функционирование системы правового регулирования обеспечения информационной безопасности, например Федеральный Закон Российской Федерации "О защите детей от информации, причиняющей вред их здоровью и развитию".
3. **Нормативно-технический**. На данном уровне осуществляется разработка стандартов, руководящих и методических материалов и документов, регламентирующих процессы разработки, внедрения и эксплуатации средств обеспечения информационной безопасности. Проводится приведение в соответствие национальных и международных стандартов в сфере информационных технологий.
4. **Административный**. Осуществление мероприятий по обеспечению безопасности на данном уровне проводится в рамках конкретного предприятия, учреждения, организации. На этом уровне руководство организации реализует конкретные меры по обеспечению информационной безопасности. В их основе лежит политика безопасности предприятия (совокупность документированных управленческих решений, направленных на защиту информации), определяющая стратегию предприятия в области информационной безопасности, а также объем выделяемых ресурсов для создания и функционирования системы комплексного обеспечения информационной безопасности.
5. **Программно-технический уровень**. Данный уровень предполагает использование как программных, так и технических средств для обеспечения информационной безопасности, среди них: идентификация и проверка подлинности пользователей средств информатизации; управление доступом к информации; протоколирование и аудит; криптография; экранирование; обеспечение высокой доступности и т.п.

Проблема защиты детей от вредной информации напрямую связана с темой образования. Формирование у учащихся умений работать с информацией и, следовательно, умений обеспечения ее безопасности, является важной задачей образования. Сегодня важно не просто осознать степень нависшей над обществом опасности, но и, выявив угрозы информационной безопасности молодежи, определить, какими средствами можно их предотвратить. Проблема обеспечения информационной безопасности школьников, молодежи является в последнее время очень актуальной. В связи с этим вопрос безопасности личной информационной среды (ЛИС) каждого школьника является важной частью обеспечения безопасности всей информационно-образовательной среды.

К **факторам** информационной среды, которые могут нести в себе угрозу информационной безопасности школьников, следует отнести следующие:

1. Доступность, неподконтрольность, неограниченный объем поступления циркулирующей информации к школьникам.
2. Наличие в информационной среде модифицированных физических носителей информации, воздействующих на физиологические системы ребенка.
3. Наличие в информационных потоках специфических элементов, целенаправленно изменяющих психофизиологическое состояние детей и подростков.

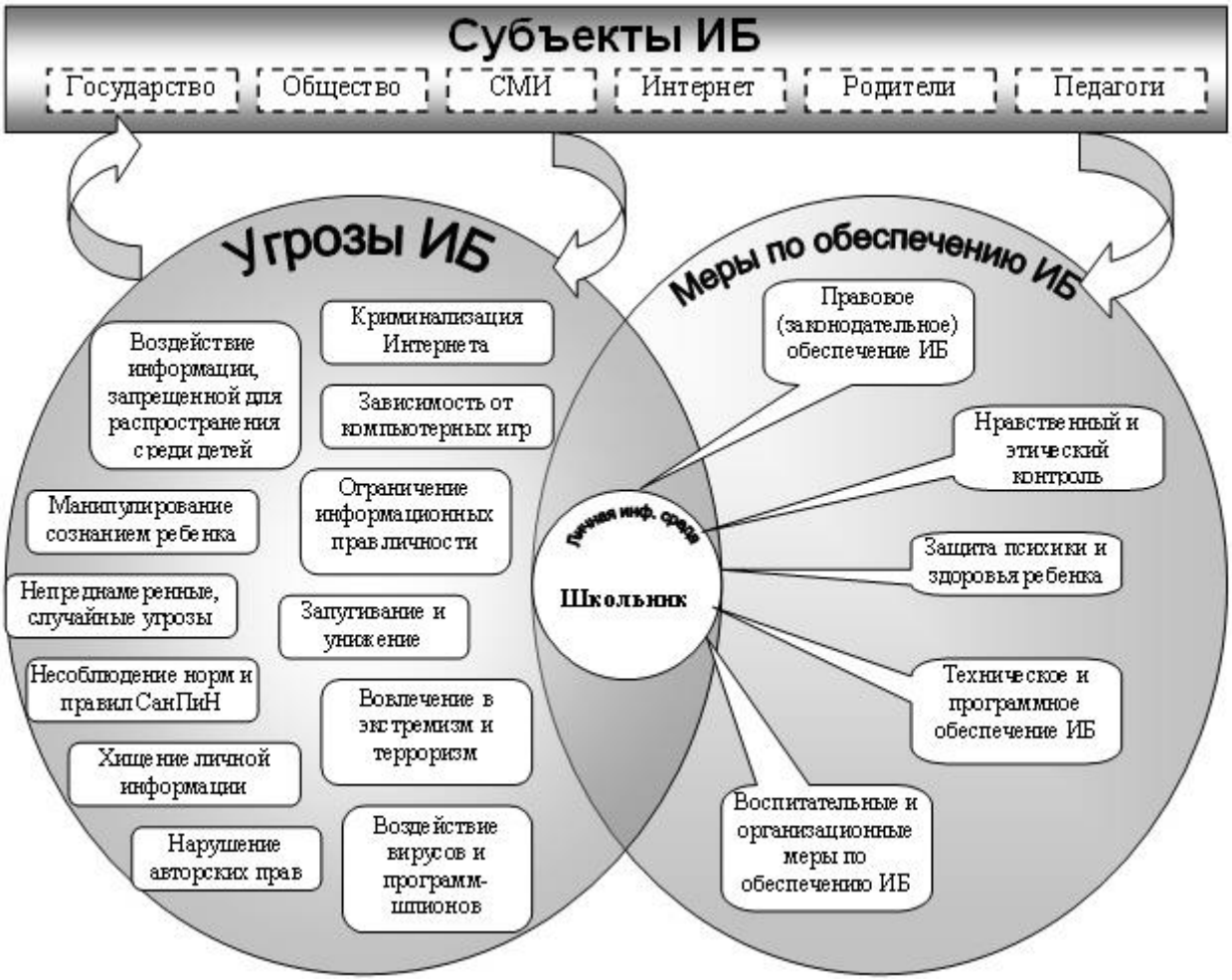
4. Наличие в информационной среде информации манипулятивного характера, дезориентирующих школьников, ограничивающих их возможности в условиях слабой правовой образованности и в силу возрастных особенностей несовершеннолетних.

Угроза - это потенциальные или реальные действия, приводящие к моральному или материальному ущербу. Угрозы могут быть как реальными, т. е. уже проявившимися в своем негативном, разрушительном воздействии на объект безопасности, так и потенциальными, т. е. их негативное воздействие может проявить себя в ближайшем или отдаленном будущем. Общая структура угрозы складывается из объекта угрозы, ее источника и проявления угрозы.

Представим угрозы информационной безопасности (ИБ) детей как совокупность условий и факторов, воздействующих на здоровье ребенка, его духовно-нравственную сферу, межличностные отношения, создающих опасность жизненно важным интересам личности в социальном, психологическом и педагогическом аспектах. Классифицируем угрозы безопасности детей и сгруппируем их по следующим направлениям: нравственные (идеологические), психофизиологические и угрозы потери информации и материального ущерба.

Информационные опасности современных школьников - это негативная сторона перехода к информационному обществу, формирующееся под воздействием вышеуказанных информационных угроз и рисков, которым современный школьник должен уметь противостоять, организовывая свою учебную деятельность.

На основе анализа и классификации факторов, рисков и угроз информационной безопасности детей была построена модель обеспечения комплексной информационной безопасности школьников (см. рис. 2.1).



увеличить изображение

Рис. 2.1. Модель обеспечения информационной безопасности школьников

Целью и результатом реализации данной модели служит формирование информационно-безопасной личности выпускника. **Объектом информационной безопасности** в данной модели является личная информационная среда (ЛИС) школьника. В условиях школьного образования обеспечение информационной

безопасности ЛИС учащихся предлагается рассматривать как совокупность деятельности по недопущению вреда здоровью, сознанию и психике ребенка.

Не менее важным вопросом при построении модели ИБ школьников является определение **субъектов информационной безопасности** - то есть тех, кто влияет на информационную безопасность школьников и несет ответственность за ее обеспечение. Существуют уровни субъектов ИБ, а именно: государство, общество, личность (см. рис. 2.1). На уровне государства должно быть осуществлено нормативно-правовое регулирование вопросов информационной безопасности несовершеннолетних, организовано "обеспечение информационной безопасности и централизированной фильтрации несовместимого с учебным процессом контента", организовано обновление содержания учебных программ, учебников по вопросам безопасности Интернета в курсе информатики.

На уровне общества действуют следующие субъекты: общественные и коммерческие организации, религиозные организации, средства массовой информации (телевидение, радио, печатные издания, Интернет), общеобразовательные учебные заведения, родители.

С учетом зарубежного и отечественного опыта информационной безопасности субъекты информационной безопасности должны осуществлять **меры** по обеспечению безопасности личной информационной среды школьника в рамках следующих направлений:

Правовое обеспечение информационной безопасности - это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту личной информационной среды учащегося на законодательной и правовой основе для реализации единой государственной политики в сфере защиты детей от информации, причиняющей вред их здоровью и развитию.

Нравственный и этический контроль подразумевает соблюдение школьниками при осуществлении информационной деятельности норм и правил поведения в обществе, а также сетевой культуры и этики, которые складываются по мере распространения информационных технологий в современном информационном обществе.

Защита психики и здоровья ребенка. Меры направлены на актуализацию потребности школьников в хорошем здоровье, физическом благополучии как средств достижения жизненно важных ценностей, снижение и профилактика компьютерной и интернет-зависимости среди учащихся, педагогическая и психологическая помощь в вопросах уменьшения информационных опасностей в жизнедеятельности школьников.

Организационная защита - это регламентация информационной деятельности подростков, контроль использования сетевых сервисов и сообществ, исключающие или ослабляющие нанесение вреда ЛИС школьника.

Воспитательные меры по обеспечению ИБ. Необходимо формировать у подрастающего поколения культуру безопасности, ответственность за осуществленные действия в информационном пространстве, воспитывать и укреплять духовно-нравственные ценности, патриотизм, готовить родителей и педагогов к принятию позиции ребенка и уважению его самостоятельности.

Техническое и программное обеспечение ИБ - это использование различных аппаратных и программных средств, препятствующих нанесению материального или морального ущерба личной информации, программ родительского контроля, сетевых фильтров, технических средств защиты информации.

Представленные меры по обеспечению информационной безопасности подрастающего поколения должны быть обусловлены прежде всего возрастными, психологическими и физиологическими особенностями школьника как формирующейся личности и тем, что он, в сравнении с представителями других социальных групп, в большей степени подвержен негативному воздействию информации, наносящей вред его нравственному развитию и здоровью.

В национальной стратегии действий в интересах детей, подписанной Президентом Российской Федерации в 2012 году, также перечислены меры, направленные на обеспечение информационной безопасности детства.

1. Создание и внедрение программ обучения детей и подростков правилам безопасного поведения в интернет-пространстве, профилактики интернет-зависимости, предупреждения рисков вовлечения в противоправную деятельность, порнографию, участию во флэшмобах.
2. Создание правовых механизмов блокирования информационных каналов проникновения через источники массовой информации в детско-подростковую среду элементов криминальной психологии, культа насилия, других откровенных антиобщественных тенденций и соответствующей им атрибутики.

3. Внедрение системы мониторинговых исследований по вопросам обеспечения безопасности информационно-образовательной среды образовательных учреждений, а также по вопросам научно-методического и нормативно-правового обеспечения соблюдения санитарно-гигиенических требований к использованию информационно-компьютерных средств в образовании детей.
4. Создание общественных механизмов экспертизы интернет-контента для детей.
5. Создание порталов и сайтов, аккумулирующих сведения о лучших ресурсах для детей и родителей; стимулирование родителей к использованию услуги "Родительский контроль", позволяющей устанавливать ограничения доступа к сети Интернет.

   Таким образом, можно констатировать, что проблема обеспечения информационной безопасности школьников является не столько социальной, сколько психолого-педагогической проблемой, так как напрямую зависит от уровня и качества нравственной культуры и воспитания подрастающего поколения. То есть перед образованием в целом и предметным обучением стоит задача сформировать интеллектуально-духовную систему личности ученика в соответствии с целями образования и обучения, а также подготовить эту систему к саморазвитию и самосовершенствованию в соответствии с ее информационными потребностями и познавательными интересами.

   Учителя и родители должны понимать, что современные дети живут в новом информационном обществе глобальной коммуникации, в котором существуют как новые возможности, так и новые угрозы и риски. И чтобы ребенок вырос конкурентоспособным гражданином, он должен постигать эти возможности. И даже если при этом ребенок столкнется с угрозами и рисками, у него будет вырабатываться своеобразный "иммунитет" на информационный негатив.

Список литературы

1. Федеральный закон от 29.12.2010 № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию". URL: www.consultant.ru.
2. Баева И.А. Психологическая безопасность образовательной среды: учеб. пособие [Текст] / Под ред. И. А. Баевой. - М., 2009. - 152 с.
3. Богатырева Ю.И. Анализ проблем информационной безопасности личности обучающихся [Текст] / Новые информационные технологии в образовании: материалы VI междунар. научно-практической конференции, Екатеринбург, 12-15 марта 2013 г. // ФГАОУ ВПО "Рос. гос. проф.-пед. ун-т", Екатеринбург, 2013. - 390 с. - С. 313-316.
4. Бочаров М.И. Комплексное обеспечение информационной безопасности школьников. [Текст] // Применение новых информационных технологий в образовании. 2009.
5. Грачев Г.В. Информационно-психологическая безопасность личности: теория и технология психологической защиты: автореф. дис. ... д-ра психол. наук. - М., 2000. С. 30.
6. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 09.09.2000 № Пр-1895) [Текст] // Российская газета, 28.09.2000, № 187.
7. Лига безопасного Интернета. URL: http://www.ligainternet.ru/news/news-detail.php?ID=2021.
8. Малых Т.А. Педагогические условия развития информационной безопасности младшего школьника: автореф. дис. ... канд. пед. наук. [Текст]. - Иркутск, 2008.
9. Национальная стратегия действий в интересах детей на 2012-2017 годы. URL: http://www.soprotivlenie.org.
10. О Стратегии национальной безопасности Российской Федерации до 2020 года. Указ Президента РФ от 12 мая 2009 г. № 537 // Российская газета, http://www.rg.ru/gazeta/rg/2009/05/19.html, № 4912.
11. Поляков В.П. Методическая система обучения информационной безопасности студентов вузов: автореф. дис. ... д-ра пед. наук. [Текст]. - Н. Новгород, 2006.
12. Привалов А.Н. Основные угрозы информационной безопасности субъектов образовательного процесса [Текст] / А.Н. Привалов, Ю.И. Богатырева // Известия Тульского государственного университета. Гуманитарные науки. - Тула, 2012. Вып. 3. - С. 427-431.
13. Портал Российской государственной детской библиотеки: научно-методический отдел.http://metodisty.rgdb.ru/articles/2063.
14. Саттарова Н.И. Информационная безопасность школьников в образовательном учреждении: дис. ... канд. пед. наук. [Текст]. - СПб., 2003.
15. Khanty-Mansiysk Autonomous Okrug - Ugra: official Site of the Public Authorities.http://www.upr.admhmao.ru/wps/wcm/connect/Web+Content/hmao-departments/chld/imayu_pravo.