
Компетентность педагогов и психологов в области информационной безопасности детей

Шпагина Е.М., кандидат психологических наук, доцент кафедры юридической психологии и права ФГБОУ ВО МГППУ, Москва, Россия (shpaginaelena@yandex.ru)

Чиркина Р.В., кандидат психологических наук, доцент, заведующая кафедрой юридической психологии и права ФГБОУ ВО МГППУ, Москва, Россия (rimtach@bk.ru)

Защищенность интересов, развития личности, здоровья и благополучия детей в информационной сфере выходит в настоящее время на первый план в связи со стремительной цифровизацией повседневной жизни. В статье рассматриваются проблемы влияния современных информационных технологий на подрастающее поколение, подходы к снижению рисков и обеспечению информационной безопасности детей, а также проблемы формирования компетентности педагогов и психологов в этой области. Перед специалистами и руководителями системы образования стоят задачи просвещения родителей и организации помощи детям в преодолении рисков и опасностей интернет среды. По мнению авторов, компетентность педагогических кадров в области обеспечения информационной безопасности детей должна складываться из комплекса знаний, включающих организационно-правовые, организационно-технические и психолого-педагогические аспекты проблемы. Основной акцент в статье сделан на правовых и психолого-педагогических аспектах информационной безопасности детей, которые определяют содержание подготовки педагогов и психологов. Представлен примерный тематический план курса повышения квалификации для руководителей и специалистов системы образования.

Ключевые слова: компетентность педагогов и психологов; информационная безопасность детей; информация, причиняющая вред здоровью и развитию детей; киберпсихология.

Для цитаты:

Шпагина Е.М., Чиркина Р.В. Компетентность педагогов и психологов в области информационной безопасности детей. [Электронный ресурс] // Психология и право. 2019(9). № 3. С. 261-277.
doi: 10.17759/psylaw.2019090319

For citation:

Shpagina E.M., Chirkina R.V. Competence of teachers and psychologists in the field of

information security of children. [Elektronnyi resurs]. Psikhologiya i pravo [Psychology and Law], 2019(9), no. 3. pp. 261-277.
doi: 10.17759/psylaw.2019090319

Цифровые информационно-телекоммуникационные технологии прочно вошли в нашу повседневную жизнь: современный мобильный телефон с выходом в сеть Интернет и соответствующими приложениями стал обязательным атрибутом людей всех возрастов. Об этом говорят не только наши наблюдения за окружающими, но и научные исследования [1; 2; 10; 11; 25; 26]. В динамике стремительного внедрения информационных технологий во все сферы жизни человека выделяют как положительные, так и отрицательные стороны цифровизации. Однако, споры о «плохом» и «хорошем» воздействии ИТ-технологий на нашу жизнь не влияют на скорость их распространения и интенсивность использования.

Ученые, общественные деятели, педагоги, родители во всем мире уже давно задаются вопросом о влиянии информационных технологий на подрастающее поколение. Не отрицая положительного влияния ИТ-технологий на развитие детей и подростков, исследователи выделяют и множество негативных эффектов, таких как: изменения качества высших психических функций (памяти, внимания, мышления), аддикция (зависимость) от гаджетов, риски влияния отрицательного по содержанию контента на психику и социализацию ребенка, а также нежелательные контакты, появляющиеся с помощью коммуникационных технологий сети Интернет. В связи с этим встает вопрос об обеспечении безопасности наших детей в новой информационной среде.

Вопросы информационной безопасности ребенка рассматривались и до бурного развития и внедрения в повседневную жизнь человека ИТ-технологий. Так, в статье 17 Конвенции о правах ребенка, ратифицированной в Советском Союзе в 1989 году, говорится о необходимости обеспечения доступа детей к информации, способствующей их воспитанию и развитию, и о запрете информации, наносящей вред.

В современной России определение информационной безопасности детей дано в п.4. ст.2. Федерального закона от 29.12.2010 N 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»: это «...состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию» [19].

В более широком смысле информационную безопасность детей можно рассматривать и как составляющую часть информационной безопасности государства [20], определение которой дается в Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента РФ от 05.12.2016 N 646: «Информационная безопасность Российской Федерации (далее - информационная безопасность) - состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства...».

Обобщая вышеуказанные определения, под информационной безопасностью ребенка следует понимать такое состояние защищенности интересов ребенка в информационной

сфере, при котором он будет, с одной стороны, иметь необходимую информацию для его полноценного обучения и развития, а с другой стороны, будет защищен от негативного воздействия информации, которая может принести ему вред.

В качестве основных направлений обеспечения информационной безопасности детей и подростков можно выделить следующие: 1) правовая защита, заключающаяся в создании нормативно-правовой базы регулирования общественных отношений в этой области; 2) технологическая защита, направленная на создание технических способов блокировки нежелательного контента, ограничения доступа к отрицательной информации, технические возможности осуществления родительского контроля за временем пребывания ребенка в сети и качественный анализ сайтов и интернет-сообществ, посещаемых детьми; 3) психолого-педагогические методы, направленные на работу с ребенком по формированию его медиа и компьютерной грамотности, стратегий поведения при встрече с нежелательным контентом и опасными знакомыми в сети Интернет, формирование критического мышления по отношению к информации, получаемой в сети и др. Наиболее эффективными признаны методы психолого-педагогического воздействия, без отрицания значения первых двух.

Однако в России программы, направленные на повышение грамотности педагогов и психологов в области обеспечения информационной безопасности детей, в настоящее время пока только разрабатываются. В связи с этим встает вопрос о содержании и границах компетентности педагогов и психологов, специалистов по работе с детьми и семьей. Что они должны знать, какой опыт иметь в этой области, чтобы противостоять «информационным» угрозам, научить и помочь справиться с возникающими проблемами детям и их родителям.

Начнем с правовых вопросов. В России базовым законодательным проектом в области регуляции вопросов информационной безопасности детей стал Федеральный закон Российской Федерации от 29 декабря 2010 г. N 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию». Данный закон определил два основных вида информации, причиняющей вред здоровью и (или) развитию детей: запрещенной для распространения среди детей и информации, распространение которой среди детей определенных возрастных категорий ограничено [19]. В Законе также рассматриваются требования к обороту информационной продукции, предназначенной для детей, и градации её в зависимости от возраста. Для введения в оборот информационной продукции данный закон обязывает проводить экспертизу информационной продукции. Проведение экспертизы требует подготовки соответствующих специалистов-экспертов в этой области.

Закон определяет государственный надзор и общественный контроль за соблюдением законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию, а также ответственность за его нарушения, предусмотренные положениями Кодекса Российской Федерации об административных правонарушениях от 30 декабря 2001 г. N 195-ФЗ (КоАП РФ) (с изменениями и дополнениями).

Принятие Закона способствовало урегулированию вопросов размещения запрещенного контента в СМИ, в первую очередь, в области телевидения и радиовещания, что было, несомненно, шагом вперед. Однако сеть Интернет трудно поддается контролю из-за своей структуры и технической организации. Сайт, просматриваемый ребенком (в том числе и на русском языке), может быть зарегистрирован в любой точке мира и не подпадать

под законодательный контроль Российской Федерации. Кроме того, все чаще говорят о так называемом «черном Интернете», где «посредством TOR пользователи Интернета могут анонимно посещать сайты, вести блоги, отправлять почтовые сообщения, а также работать с другими приложениями, использующими протокол TCP. Сохранение анонимности трафика происходит за счет использования распределенной сети» [15, с.650]. Найти инструкцию (в том же Интернете) по использованию технологии TOR может любой продвинутый школьник. Однако найти и привлечь к ответственности того, кто размещает запрещенную информацию, технически очень трудно. Преступники используют данную технологию достаточно активно. Р.М. Узденов в статье «Новые границы киберпреступности» выделяет девять направлений использования анонимного интернета преступниками всех специализаций [15]. Многие из этих направлений имеют четкую ориентацию на детей и подростков. Проблемы законного «обуздания» анонимного Интернета характерны для всего мирового сообщества.

И.М. Рассолов выделяет основные проблемы судебной практики: «1) сложность определения круга лиц, привлекаемых к юридической ответственности и обязанных компенсировать моральный вред и материальный ущерб пострадавшему; 2) фиксация (сбор, представление) доказательств, их допустимость и достоверность» [12, с.103].

Принятые в недавнем прошлом новые документы в области информационных технологий и информационной безопасности, такие как Доктрина информационной безопасности РФ (утв. Указом Президента РФ от 5 декабря 2016 г. № 646) и Стратегия развития информационного общества на 2017 – 2030 годы (утв. Указом Президента РФ от 9 мая 2017 г. N 203) [5; 14], только декларируют основные направления развития информационного общества и вопросы кибербезопасности в России, но не дают конкретных разъяснений алгоритмов осуществления информационной безопасности личности, общества и государства. Правовому (юридическому) сообществу придется повернуться лицом к новым информационным технологиям, чтобы держать руку на пульсе регулирования правовых норм в этой области.

Концепция информационной безопасности детей, утвержденная распоряжением Правительства Российской Федерации от 2 декабря 2015 года № 2471-р, содержит основные направления обеспечения информационной безопасности детей в России. Наряду с тем, что в Концепции предусматриваются психолого-педагогические меры, направленные на формирование механизмов защиты детей от информации, наносящей вред их здоровью и развитию, главный акцент направлен на поддержку и совершенствование механизмов блокировки сайтов в сети «Интернет», содержащих включение их в Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в РФ запрещено на основании трех законов Российской Федерации: «О защите детей от информации, причиняющей вред их здоровью и развитию», «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации» и Федерального закона «О лотереях» [16; 19; 20].

Другой очень важный юридический вопрос, связанный с обеспечением информационной безопасности детей, - защита персональных данных [22]. Педагоги и психологи, по роду деятельности, постоянно имеют дело с персональными данными. Цифровизация, в том числе воспитательного и образовательного процесса, приводит к

появлению различных информационных ресурсов, содержащих персональные данные, личную информацию детей. Однако уровень компетентности специалистов, работающих с детьми, в области обращения с персональными данными, часто оставляет желать лучшего. Специальное обучение в этой области для педагогов и психологов отсутствует. С одной стороны, цифровые технологии упрощают возможности анализа и обобщения информации, помогают в управлении и планировании, с этим трудно поспорить. Но тогда нужно учить рядового пользователя (в нашем случае педагога и психолога) вопросам защиты информации, в первую очередь, персональных данных детей. Потребность в этом, например, подтверждается появлением Федерального закона от 16.04.2001 N 44-ФЗ «О государственном банке данных о детях, оставшихся без попечения родителей», где в ст. 4 обязательным требованием к формированию и использованию государственного банка данных о детях прописано «обеспечение безопасности документированной информации при ее обработке, в том числе принятие необходимых правовых, организационных и технических мер для защиты документированной информации от неправомерного или случайного доступа к ней, уничтожения, изменения, блокирования, копирования, предоставления, распространения и иных неправомерных действий в отношении документированной информации (в ред. Федерального закона от 07.05.2013 N 99-ФЗ)»[17]. Вместе с тем тенденция к расширению подобных информационных ресурсов предъявляет новые требования к повышению компетентности всех специалистов и руководителей системы образования в области защиты информации.

Техническая сторона вопроса (лучше сказать организационно-техническая, потому что педагог и психолог не являются техническими специалистами) защиты детей от информации, наносящей вред их здоровью и развитию, вытекает из юридической. Как оградить ребенка от нежелательного контента? Как защитить конфиденциальную информацию (например, персональные данные)? В каких условиях её можно обрабатывать?

На сегодняшний день, наиболее распространенным способом обеспечения информационной безопасности детей от нежелательного контента является способ фильтрации, создание программ типа «родительский контроль». Наиболее продвинулась в этой области в нашей стране, на наш взгляд, «Лаборатория Касперского», которая занимается вопросами информационной безопасности детей на протяжении многих лет и имеет набор не только средств защиты информации, но и опыт просвещения детей родителей и педагогов в этой области. На Интернет-страницах Лаборатории Касперского [6] размещены статьи различных специалистов, обучающие материалы и мультфильмы, повествующие в популярной форме об основных угрозах информационной безопасности и способах противодействия им.

Компетентность педагогов и психологов в области организационно-технической защиты информации должна касаться таких вопросов как:

- 1) условия обработки информации ограниченного доступа (персональные данные, медицинская информация и другая);
- 2) элементарные знания в области защиты информации в компьютере;
- 3) обеспечение безопасности информации при работе с интернетом;
- 4) осведомленность о программах «родительский контроль» и их функциях;

-
- 5) элементарные знания о возможностях «пожаловаться» или заблокировать нежелательный контент в социальных сетях, правилах безопасности в социальных сетях.

Этот список будет расширяться по мере развития технологий, что потребует изменения психологии «гуманитария» и обращения к современным техническим средствам общения и выражения себя, какими еще недавно были ручка и бумага.

И ещё одно направление защиты детей от негативной информации в Интернете лежит в социальной, психологической, педагогической плоскостях и наиболее развито в мировой практике. Суть данного направления в подготовке детей к осознанной встрече с информационными угрозами. Родители, педагоги, общественность и даже провайдеры берут инициативу на себя и предлагают взять проблему информационной безопасности детей под свой контроль, предлагая психолого-педагогические меры защиты.

Интересен опыт в этой области некоторых зарубежных стран. Так, например, Г.В. Михалева в своей работе раскрывает основные навыки медиакомпетенций, которые приведены в Современной британской стратегии медиапросвещения, которая рекомендует:

1) научить детей удовлетворять индивидуальные или общественные потребности и интересы в информационной сфере, используя современные технологии для обеспечения основных информационных процессов: доступа, получения, хранения, восстановления, извлечения и обмена информацией;

2) сформировать умение делать оптимальный и необходимый по содержанию выбор информации из большого числа видов медиа и медиатекстов из различных источников, относящихся к разнообразным культурам и институтам;

3) научить детей пониманию цели и механизмов создания медиатекстов;

4) сформировать навык критического анализа языка и условных кодов, приемов, используемых в медиа для передачи информации и сообщений;

5) научить детей самовыражению путем творческого использования медиа путем трансформации и передачи идей, сведений и мнений;

6) обучать детей критически оценивать, распознавать и избегать агрессивную и опасную информацию или услуги;

7) уметь эффективно использовать информационные технологии и медиа в качестве инструмента осуществления демократических прав и гражданских обязанностей» [8, с.35].

Опыт Франции в этой сфере представлен в работе О.П. Юрченко [24]. «Эволюции идеи защиты детей от вредного воздействия медиа в диапазоне от «запретить, значит, защитить» до «подготовить к критическому восприятию медиасообщений, значит, вооружить» в большей степени способствовала деятельность французских медиапедагогов Центра связи образования и средств информации (CLEMI – Le Centre de liaison de l'enseignement et des médias d'information) [24, с.303]. Данный проект под названием «Неделя прессы в школе», осуществляемый под надзором Министерства образования Франции направлен на формирование навыков восприятия и использования информации разных медиа (пресса,

телевидение, радио), передаваемых, в том числе, в современных условиях посредством сети Интернет. Акцент делается не на защитных и запретительных мерах. Речь идет о формировании культуры выбора контента и критического отношения к нему у детей и подростков. В своей работе автор отмечает, что в России государственная образовательная политика очень мало охватывает сферу медиаобразования, делая ссылку на Государственную программу РФ «Развитие образования» на 2013–2020 гг.

Об образовательных мерах в области информационной безопасности детей говорит в своей работе Д.А.Герасимов [4, с.144]. Исследования онлайн-угроз несовершеннолетним в США в 2008 году обнаружили следующие факты:

1) интернет-риски в виде сексуальных домогательств и кибербуллинг в отношении подростков и детей;

2) опасность за пределами Сети («оффлайн») гораздо больше, чем реальная угроза в Интернете;

3) регулярные меры по воспитанию, общение с ребенком родителей и учителей помогают преодолеть угрозы Интернета намного лучше, чем всевозможные технологии фильтрации;

4) технологии (фильтры, маркировки) не смогут избавить на 100 % детей и подростков от возможных опасностей в Сети

В России существует несколько некоммерческих проектов, направленных на обеспечение информационной безопасности детей в сети Интернет: «Дети России онлайн», «Фонд развития Интернета», «Академия Касперского», «Лига безопасного Интернета», «Безопасность детей в Интернете», проект Google «Сделайте Интернет безопасным для своих детей», Общероссийское детское общественное движение в сфере обеспечения безопасности и развития детей в информационном пространстве «Страна молодых» и ряд других. Наиболее известный проект по информационной безопасности детей осуществлен на Факультете психологии МГУ имени М.В. Ломоносова под руководством Г.У. Солдатовой при содействии Фонда развития интернет. Результаты исследования, которые были созвучны исследованиям, проводимым в Европе под руководством Сони Левингстон [26], показали, что Интернет-среда является одним из основных инструментов социализации в молодежной среде и средством формирования идентичности и «цифрового гражданства»: «Цифровая компетентность включает в себя не только знания и умения, но и другие важные компоненты: мотивацию человека на развитие и его ответственность как гражданина цифрового мира. Диагностика ответственности позволит понять отношение человека к технологиям, его ценности и готовность занимать гражданскую позицию в цифровом мире. Мотивация же определяет развитие его цифровой компетентности в будущем» [22, с.135].

Результаты данного исследования показали, что наиболее эффективным способом осуществления информационной безопасности детей и подростков, с психологической точки зрения, является обсуждение и разъяснение (медиация) детям опасностей и способов избежать последствия этих угроз в интернете и в жизни. По данным исследований, при таком подходе, дети чаще обсуждают с родителями проблемы, с которыми они столкнулись в Интернете, меньше тревожатся и испытывают страх при встрече с негативной

информацией (изображение сексуального характера, получение сообщения сексуального характера, негативный контент, общение с интернет-знакомыми) [13].

Содержание компетенций в области информационной безопасности детей далеко не исчерпывается перечисленными выше и постоянно расширяется, так же быстро, как и влияние Интернета и информационных технологий на нашу жизнь.

Несмотря на признание проблемы информационной безопасности детей российскими общественными и правовыми институтами, данный вопрос требует тщательной проработки и развития во всех описанных выше направлениях: организационно-правовом, техническом и социально-психолого-педагогическом уровнях. Одним из пусковых механизмов формирования комплексной системы информационной безопасности детей может быть создание обучающих программ в этой области для педагогов и психологов, работающих с детьми и их родителями.

Такие шаги предпринимаются, например, на сайте www.единьурок.рф, который предлагает повысить квалификацию по программам: 1) «Безопасное использование сайтов в сети «Интернет» в образовательном процессе в целях обучения и воспитания обучающихся в образовательной организации»; 2) «Основы обеспечения информационной безопасности детей»; 3) «Организация защиты детей от видов информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования, в образовательных организациях» [1]. Инициативу в данной области взяла на себя Временная комиссия Совета Федерации по развитию информационного общества.

Особое внимание хочется уделить третьему направлению повышения квалификации (компетентности) педагогов и психологов, которая касается непосредственно их сферы деятельности: это психолого-педагогические методы обеспечения информационной безопасности детей.

А.В. Федоров в своей монографии рассматривает вопросы развития медиакомпетентности и критического мышления студентов педагогического вуза, где цитирует британского педагога-исследователя в области медиа Д. Букингэма (D.Buckingham): «Эпоха «информационного общества» привела к «появлению новой парадигмы медиаобразования. Медиаобразование видится не формой защиты, но формой подготовки» [19].

В России существует потребность в создании программ и проектов, связанных с образованием в области психологической безопасности в работе с информационными технологиями для трех категорий: детей, родителей и лиц, которые занимаются с детьми профессионально: руководителей образования, педагогов, психологов.

Изменение психологической реальности, связанной с внедрением интернет технологий в повседневную жизнь, требует новых подходов к обучению специалистов, работающих с детьми. Информационная безопасность детей основывается на изучении социально-психологических феноменов, которые претерпели изменения под воздействием технологий и требуют нового переосмысления. Методологическая основа разработки такого обучения должна опираться на исследования и рекомендации специалистов в этой области.

Обобщая материалы исследований, можно разделить психологические феномены и явления, связанные с влиянием технического прогресса и внедрением информационно-коммуникационных технологий в повседневную жизнь, на две основные категории:

1) влияние технологий на высшие психические функции: память, внимание, восприятие и мышление в целом, речь;

2) социально-психологические явления, такие как феномены изменения идентичности человека, появление виртуальных сообществ и групп и их влияние на личность, такие формы агрессивного поведения, как кибербуллинг, использование Интернета для реализации насильственных действий в реальности и т.д. Вызывает тревогу такое явление, как киберзависимость, в том числе и с самого раннего возраста, когда у детей формируется стойкая зависимость эмоционального состояния от гаджетов.

Все эти явления все чаще становятся предметом изучения психологического сообщества и требуют новых подходов к осмыслению влияния технического прогресса на психику человека, выработке методов диагностики и профилактики негативного влияния ИТ, а также включения психологических знаний в разработку новых технологий, не причиняющих вред, а развивающих и улучшающих благополучие и качество жизни.

В связи с этим, предлагаем следующий тематический план курса повышения квалификации для педагогов и психологов, который затрагивает социально-психологические феномены информационной безопасности личности:

1) Введение в дисциплину, методология, междисциплинарные связи. Актуальность изучения дисциплины. Понятие - информационная безопасность детей.

2) История развития киберпсихологии. Компьютерная психология. Виртуальная психология. Киберпсихология.

3) Основополагающие психологические теории и исследования, лежащие в основе информационных процессов. Когнитивная психология. Психологические особенности получения, обработки, хранения, передачи и воздействия информации. Роль информации в принятии решений. Искусственный интеллект.

4) Социально-психологические теории, используемые в объяснении поведения человека во взаимодействии с технологиями.

5) Влияние технического прогресса и стремительное развитие ИТ-технологий на высшие психические функции. Влияние использования технологий на память, внимание, восприятие и в целом, на мышление. Возможности и ограничения образовательных процессов с помощью ИТ-технологий.

6) Социально-психологические аспекты влияния ИТ-технологий. Изменение идентичности личности. Изменение параметров общения, особенности сетевого общения. Киберсоциализация. Виртуальные киберсообщества.

7) Интернет-риски: контентные; нежелательное знакомство, секстинг и грумминг; кибербуллинг.

8) Интернет-аддикция и компьютерная зависимость. Компьютерная зависимость как форма аддикции. Критерии диагностики компьютерной зависимости. Методы профилактики и лечения компьютерной зависимости.

9) Возможности диагностики и проведения исследований влияния технического прогресса на деятельность человека. Возможности диагностики с помощью IT-технологий. Диагностика изменений высших психических функций. Диагностика интернет-зависимости. Диагностика изменения идентичности личности. Диагностика психических состояний посредством поведения в сети. Диагностика (профайлинг) личности пользователя сети.

10) Экспертиза информационной продукции и выявление информации, наносящей вред их здоровью и развитию. Юридические основания проведения экспертизы. Маркировка информационной продукции. Методика проведения экспертизы информационной продукции. Перспективы развития экспертизы информационной продукции. Подготовка специалистов.

11) Возможности и перспективы обеспечения информационной безопасности детей с помощью психолого-педагогических методов и технологий. Психологическое обоснование ограничений и доступа детей к пользованию IT-технологиями согласно их возрасту и развитию. Приоритет развития ребенка с позиции культурно-исторического подхода и предметной деятельности. Цифровая компетентность детей и родителей. Разработка методов профилактики Интернет-рисков с участием родителей, педагогов и детей. Формирование медиакомпетентности и критического мышления к продукции СМИ у детей среднего и старшего школьного возраста (подростков и молодежи).

Данная тематика не является исчерпывающей, а курс повышения квалификации требует дальнейшей содержательной проработки и развития.

В заключение следует отметить, что поскольку вопросы информационной безопасности детей с внедрением информационных технологий в повседневную жизнь стали достаточно актуальными, необходимо на уровне государственной политики и на уровне всех институтов социализации уделять внимание вопросам обучения детей в области информационной безопасности. Меры противостояния информационным угрозам лежат в разных плоскостях: юридическая область, организационно-техническое и психолого-педагогическое направление. Система обучения противостояния угрозам информационной безопасности прошла путь от идеи запретов к идее формирования критического мышления ребенка. Дети и подростки в таком подходе рассматриваются как сознательные пользователи информации, которые могут ориентироваться в информационном потоке и делать осознанный выбор, умеют выражать себя через информационные технологии. Для достижения этого необходимы специальные обучающие программы и педагоги, обладающие знаниями в области информационной безопасности детей.

Литература

1. Безопасное использование сайтов в сети «интернет» в образовательном процессе в целях обучения и воспитания обучающихся в образовательной организации [Электронный ресурс]: Портал «Единыйурок.рф» // URL: <https://www.xn--d1abkefqip0a2f.xn--p1ai/index.php/kartochka-programmy/item/603-formirovanie-i-razvitiie-pedagogicheskoi-ikt-kompetentnosti-v-sootvetstvii-s-trebovaniyami-fgos-i-professionalnogo>

- standarta (дата обращения: 11.06.2019).
2. Будыкин С.В. Информационная безопасность детей и подростков в современном мире: психологические аспекты проблемы [Электронный ресурс] // Психология и право. 2017. Том 7. № 1. С. 13–24. doi:10.17759/psylaw.2017070102
 3. Будыкин С.В., Дворянчиков Н.В., Бовина И.Б. Информационная безопасность детей и подростков в понимании родителей и учителей (Часть 2. Результаты эмпирического исследования) [Электронный ресурс] // Психология и право. 2016. Том 6. № 1. С. 25–38. doi:10.17759/psylaw.2016060104
 4. Герасимов Д.А. Правовое регулирование защиты несовершеннолетних от негативного воздействия СМИ и сети интернет в США // Вестник финансового университета. 2013. №1. С.141-145.
 5. Доктрина информационной безопасности РФ (утв. Указом Президента РФ от 5 декабря 2016 г. № 646) [Электронный ресурс] // URL: <http://base.garant.ru/71556224/> (дата обращения: 26.07.2019).
 6. Защита детей в Интернете [Электронный ресурс]: Сайт Лаборатории Касперского // URL: <https://www.kaspersky.ru/resource-center/preemptive-safety/kids-online-safety> (дата обращения: 11.06.2019).
 7. Концепция информационной безопасности детей (утв. распоряжением Правительства Российской Федерации от 2 декабря 2015 года № 2471-р) [Электронный ресурс] // URL: http://www.consultant.ru/document/cons_doc_LAW_190009/(дата обращения: 26.07.2019).
 8. Михалева Г. В. Современная британская стратегия информационной безопасности детей и молодежи [Электронный ресурс] // Вестник ЧелГУ. 2013. №22 (313). URL: <https://cyberleninka.ru/article/n/sovremennaya-britanskaya-strategiya-informatsionnoy-bezopasnosti-detey-i-molodezhi> (дата обращения: 12.05.2019).
 9. Пимонов В.А. Основные проблемы обеспечения информационной безопасности субъектов образовательного процесса [Электронный ресурс] // Психология и право. 2011. № 4. URL: <http://psyjournals.ru/psyandlaw/2011/n4/49302.shtml> (дата обращения: 26.07.2019).
 10. Письмо Минпросвещения России от 07.06.2019 N 04-474 «О методических рекомендациях» (вместе с «Методическими рекомендациями по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования») [Электронный ресурс] // URL: http://www.consultant.ru/document/cons_doc_LAW_328805/ (дата обращения: 26.07.2019).
 11. Практическая психология безопасности. Управление персональными данными в интернете: учеб.-метод. пособие для работников системы общего образования / Солдатова Г.У., Приезжева А.А., Олькина О.И., Шляпников В.Н. – М.: Генезис, 2017. 224 с.
 12. Рассолов И.М. Правовые проблемы обеспечения информационной безопасности: юридическая ответственность операторов связи // Вестник Московского университета МВД России. 2013. № 12. с.103-108.
 13. Солдатова Г.У., Рассказова Е.И. Безопасность подростков в Интернете: риски, совладание

- и родительская медиация // Национальный психологический журнал, 2014. №3(15). С.39-51.
14. Стратегия развития информационного общества на 2017 – 2030 годы (утв. Указом Президента РФ от 9 мая 2017 г. N 203) [Электронный ресурс] // URL: http://www.consultant.ru/document/cons_doc_LAW_216363/e91cc5f89aaced60e19c6c6554fc03432f4ee971/ (дата обращения: 11.06.2019).
 15. Узденов Р.М. Новые границы киберпреступности // Всероссийский криминологический журнал. 2016. Т. 10. № 4. С. 649-655.
 16. Федеральный закон от 11 ноября 2003 г. N 138-ФЗ (ред. от 18.07.2019) «О лотереях» [Электронный ресурс] // URL:http://www.consultant.ru/document/cons_doc_LAW_44970/(дата обращения: 11.06.2019)
 17. Федеральный закон от 16.04.2001 N 44-ФЗ (ред.15.09.2015) «О государственном банке данных о детях, оставшихся без попечения родителей» [Электронный ресурс] // URL: <http://www.consultant.ru/cons/cgi/online.cgi?base=LAW;n=148667;req=doc#012547186619840034> (дата обращения: 11.06.2019)
 18. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 30.06.2018) «О персональных данных» [Электронный ресурс] // URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 11.06.2019)
 19. Федеральный закон от 29.12.2010 N 436-ФЗ (ред. от 18.12.2018) «О защите детей от информации, причиняющей вред их здоровью и развитию» [Электронный ресурс] // URL:http://www.consultant.ru/document/cons_doc_LAW_108808/ (дата обращения: 11.06.2019).
 20. Федеральный закон от 29 декабря 2006 N 244-ФЗ (ред. 14.07.2019) «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации» [Электронный ресурс] // URL: <https://nalogcodex.ru/laws/Federalnyy-zakon-ot-29.12.2006-N-244-FZ/> (дата обращения 11.06.2019).
 21. Федоров А.В. Развитие медиакомпетентности и критического мышления студентов педагогического вуза. М.: Изд-во МОО ВПП ЮНЕСКО «Информация для всех». 2007. 616 с.
 22. Цифровая компетентность подростков и родителей. Результаты всероссийского исследования / Солдатов Г.У., Нестик Т.А., Рассказова Е.И., Зотова Е.Ю. – М.: Фонд Развития Интернет. 2013. 144 с.
 23. Шпагина Е.М. Информационная безопасность в контексте защиты прав детей в Российской Федерации [Электронный ресурс] // Психология и право. 2016. Том 6. № 4. С. 86–94. doi:10.17759/psylaw.2016060409
 24. Юрченко О.П. Вопросы информационной безопасности школьников в теории и практике современного французского медиаобразования // Вестник Челябинского государственного университета. 2013. № 22 (313). Филология. Искусствоведение. Вып. 81. С. 302–305. 98

25. O'Neill B., Staksrud E. Final recommendations for policy. London: EU Kids Online, LSE, 2014. p.42.
URL: <http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20III/Reports/D64Policy.pdf>
26. Livingstone S., Cagiltay K., Ólafsson K. EU Kids Online II Dataset: A cross-national study of children's use of the Internet and its associated opportunities and risks/ British Journal of Educational Technology. Vol 46. No 5, 2015. P. 988-992 doi:10.1111/bjet.12317

Competence of Teachers and Psychologists in the Field of Information Security of Children

Shpagina E. M., Candidate of psychological Sciences, associate Professor, Department of legal psychology and law, Moscow, Russia (shpaginaelena@yandex.ru)

Chirkina R. V., Candidate of psychological Sciences, associate Professor, head of the Department of legal psychology and law, Moscow, Russia (rimmach@bk.ru)

Protection of interests, personal development, health and well-being of children in the information sphere is now coming to the fore in connection with the rapid digitalization of everyday life. The article deals with the problems of influence of modern information technologies on the younger generation, approaches to risk reduction and information security of children, as well as the problems of formation of competence of teachers and psychologists in this area. Specialists and managers of the education system are faced with the task of educating parents and helping children to overcome the risks and dangers of the Internet environment. According to the authors, the competence of teachers in the field of information security of children should consist of a set of knowledge, including organizational, legal, organizational, technical, psychological and pedagogical aspects of the problem. The main focus of the article is on the legal, psychological and pedagogical aspects of information security of children, which determine the content of training of teachers and psychologists. An approximate thematic plan of the training course for managers and specialists of the education system is presented.

Keywords: competence of teachers and psychologists; information security of children; information harmful to health and development of children; cyberpsychology.

References

1. Bezopasnoe ispol'zovanie saitov v seti «internet» v obrazovatel'nom protsesse v tselyakh obucheniya i vospitaniya obuchayushchikhsya v obrazovatel'noi organizatsii [Elektronnyi resurs] [Safe use of Internet sites in the educational process for the purpose of training and education of students in an educational organisation]: Portal «Edinyurok.rf». URL: <https://www.xn--d1abkefqip0a2f.xn--p1ai/index.php/kartochka-programmy/item/603-formirovanie-i-razvitie-pedagogicheskoy-ikt-kompetentnosti-v-sootvetstvii-s-trebovaniyami-fgos-i-professionalnogo-standarta> (Accessed 11.06.2019).
2. Budykin S.V. Informatsionnaya bezopasnost' detei i podrostkov v sovremennom mire: psikhologicheskie aspekty problemy [Elektronnyi resurs] [Information security of children and adolescents in the modern world: psychological aspects of the problem]. Psikhologiya i pravo [Psychology and law]. 2017. Tom 7. no. 1. pp. 13–24. doi:10.17759/psylaw.201707010. (In Russ., abstr. in Engl.).
3. Budykin S.V., Dvoryanchikov N.V., Bovina I.B. Informatsionnaya bezopasnost' detei i podrostkov v ponimanii roditelei i uchitelei (Chast' 2. Rezul'taty empiricheskogo

-
- issledovaniya) [Elektronnyi resurs] [Information security of children and adolescents as a result of understanding by parents and teachers (Part 2. Results of an empirical study)]. *Psikhologiya i pravo* [Psychology and law]. 2016. Tom 6. no. 1. pp. 25–38. doi:10.17759/psylaw.2016060104. (In Russ., abstr. in Engl.).
4. Gerasimov D.A. Pravovoe regulirovanie zashchity nesovershennoletnikh ot negativnogo vozdeistviya SMI i seti internet v SShA [Legal regulation of the protection of minors from the negative impact of the media and the Internet in the United States]. *Vestnik finansovogo universiteta* [Bulletin of Financial University]. 2013. no. 1. pp. 141-145. (In Russ., abstr. in Engl.).
 5. Doktrina informatsionnoi bezopasnosti RF (utv. Ukazom Prezidenta RF ot 5 dekabrya 2016 g. no. 646) [Elektronnyi resurs] [Information Security Doctrine of the Russian Federation (approved by Decree of the President of the Russian Federation from December 5, 2016. No. 646)]. URL: <http://base.garant.ru/71556224/> (Accessed 26.07.2019).
 6. Zashchita detei v Internete [Elektronnyi resurs][Protecting children on the Internet]: Sait Laboratorii Kasperskogo [Kaspersky Lab website]. URL: <https://www.kaspersky.ru/resource-center/preemptive-safety/kids-online-safety> (Accessed 11.06.2019).
 7. Kontseptsiya informatsionnoi bezopasnosti detei (utv. rasporyazheniem Pravitel'stva Rossiiskoi Federatsii ot 2 dekabrya 2015 goda no. 2471-r) [Elektronnyi resurs] [The concept of children's information security (approved by the order of the Government of the Russian Federation from December 2, 2015 No. 2471-r)]. URL: http://www.consultant.ru/document/cons_doc_LAW_190009/ (Accessed 26.07.2019).
 8. Mikhaleva G. V. Sovremennaya britanskaya strategiya informatsionnoi bezopasnosti detei i molodezhi [Elektronnyi resurs] [The modern British information security strategy for children and youth]. *Vestnik ChelGU* [Bulletin of Chelyabinsk State University]. 2013. no. 22 (313). URL: <https://cyberleninka.ru/article/n/sovremennaya-britanskaya-strategiya-informatsionnoy-bezopasnosti-detey-i-molodezhi> (Accessed 12.05.2019).
 9. Pimonov V.A. Osnovnye problemy obespecheniya informatsionnoi bezopasnosti sub"ektov obrazovatel'nogo protsessa [Elektronnyi resurs] [The main problems of ensuring information security of the subjects of the educational process]. *Psikhologiya i pravo* [Psychology and law]. 2011. no. 4. URL: <http://psyjournals.ru/psyandlaw/2011/n4/49302.shtml> (Accessed 26.07.2019).
 10. Pis'mo Minprosveshcheniya Rossii ot 07.06.2019 No 04-474 «O metodicheskikh rekomendatsiyakh» (vmeste s «Metodicheskimi rekomendatsiyami po ogranicheniyu v obrazovatel'nykh organizatsiyakh dostupa obuchayushchikhsya k vidam informatsii, rasprostranyaemoi posredstvom seti «Internet», prichinyayushchei vred zdorov'yu i (ili) razvitiyu detei, a takzhe ne sootvetstvuyushchei zadacham obrazovaniya») [Elektronnyi resurs] [Letter of the Ministry of Education of Russia from 07.06.2019 No 04-474 “On Methodological Recommendations” (together with the “Methodological Recommendations on restricting students' access in educational organisations to the

- types of information disseminated through the Internet that is harmful to the health and (or) development of children, as well as inadequate to education tasks”)]. URL: http://www.consultant.ru/document/cons_doc_LAW_328805/ (Accessed 26.07.2019).
11. Prakticheskaya psikhologiya bezopasnosti. Upravlenie personal'nymi dannymi v internete: ucheb.-metod. posobie dlya rabotnikov sistemy obshchego obrazovaniya [Practical safety psychology. Personal data management on the Internet: a teaching tool for employees of the general education system]. Soldatova G.U., Priezzheva A.A., Ol'kina O.I., Shlyapnikov V.N. – Moscow: Genezis, 2017. 224 pp.
 12. Rassolov I.M. Pravovye problemy obespecheniya informatsionnoi bezopasnosti: yuridicheskaya otvetstvennost' operatorov svyazi [Legal issues of ensuring information security: legal liability of telecom operators]. Vestnik Moskovskogo universiteta MVD Rossii [Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia]. 2013. no. 12. pp.103-108.
 13. Soldatova G.U., Rasskazova E.I. Bezopasnost' podrostkov v Internete: riski, sovladanie i roditel'skaya mediatsiya [Adolescent Safety on the Internet: Risks, Coping and Parental Mediation]. Natsional'nyi psikhologicheskii zhurnal [National Psychological Journal], 2014. no. 3(15). pp.39-51. (In Russ., abstr. in Engl.).
 14. Strategiya razvitiya informatsionnogo obshchestva na 2017 – 2030 gody (utv. Ukazom Prezidenta RF ot 9 maya 2017 g. No. 203) [Elektronnyi resurs] [Informational Society Development Strategy for 2017 - 2030 (approved by Decree of the President of the Russian Federation from May 9, 2017 No. 203)]. URL: http://www.consultant.ru/document/cons_doc_LAW_216363/e91cc5f89aaced60e19c6c6554fc03432f4ee971// (Accessed 11.06.2019).
 15. Uzdenov R.M. Novye granitsy kiberprestupnosti [New Borders of Cybercrime]. Vserossiiskii kriminologicheskii zhurnal [All-ussian Criminological Journal]. 2016. T. 10. no. 4. pp. 649-655. (In Russ., abstr. in Engl.).
 16. Federal'nyi zakon ot 11 noyabrya 2003 g. No. 138-FZ (red. ot 18.07.2019) «O lotereyakh» [Elektronnyi resurs] [Federal Law of November 11, 2003 No. 138- FZ (as amended on July 18, 2019) «On lotteries»]. URL:http://www.consultant.ru/document/cons_doc_LAW_44970/ (Accessed 11.06.2019).
 17. Federal'nyi zakon ot 16.04.2001 No. 44-FZ (red.15.09.2015) «O gosudarstvennom banke dannykh o detyakh, ostavshikhsya bez popecheniya roditelei» [Elektronnyi resurs] [Federal Law of 16.04.2001 No. 44-ФЗ (rev.15.09.2015) “On the state databank of children left without parental care”]. URL: <http://www.consultant.ru/cons/cgi/online.cgi?base=LAW;n=148667;req=doc#012547186619840034> (Accessed 11.06.2019).
 18. Federal'nyi zakon ot 27.07.2006 No. 152-FZ (red. ot 30.06.2018) «O personal'nykh dannykh» [Elektronnyi resurs] [Federal Law of July 27, 2006 No. 152-ФЗ (as amended on June 30, 2018) "On personal data"]. URL: http://www.consultant.ru/document/cons_doc_LAW_61801/ (Accessed 11.06.2019).

19. Federal'nyi zakon ot 29.12.2010 No. 436-FZ (red. ot 18.12.2018) «O zashchite detei ot informatsii, prichinyayushchei vred ikh zdorov'yu i razvitiyu» [Elektronnyi resurs] [Federal Law of December 29, 2010 No. 436-ФЗ (as amended on December 18, 2018) "On the protection of children from Information that harm their health and development."]. URL:http://www.consultant.ru/document/cons_doc_LAW_108808/ (Accessed 11.06.2019).
20. Federal'nyi zakon ot 29 dekabrya 2006 No. 244-FZ (red. 14.07.2019) «O gosudarstvennom regulirovanii deyatelnosti po organizatsii i provedeniyu azartnykh igr i o vnesenii izmenenii v nekotorye zakonodatel'nye akty Rossiiskoi Federatsii» [Elektronnyi resurs] [Federal Law of December 29, 2006 No. 244-ФЗ (as amended on July 14, 2019) "On state regulation of the organization and conduct of gambling and on making amendments to legislative acts of the Russian Federation"]. URL: <https://nalogcodex.ru/laws/Federalnyy-zakon-ot-29.12.2006-N-244-FZ/> (Accessed 11.06.2019).
21. Fedorov A.V. Razvitie mediakompetentnosti i kriticheskogo myshleniya studentov pedagogicheskogo vuza [The development of media competence and critical thinking of students of a pedagogical university.]. Moscow: Publ. MOO VPP YuNESKO «Informatsiya dlya vseh». 2007. 616 p.
22. Tsifrovaya kompetentnost' podrostkov i roditelei. Rezul'taty vserossiiskogo issledovaniya [Digital competence of adolescents and parents. All-Russian study results]. Soldatova G.U., Nestik T.A., Rasskazova E.I., Zotova E.Yu. – Moscow: Fond Razvitiya Internet. 2013. 144 p. Shpagina E.M. Informatsionnaya bezopasnost' v kontekste zashchity prav detei v Rossiiskoi Federatsii [Elektronnyi resurs] [Information security in the context of the protection of children's rights in the Russian Federation]. Psikhologiya i pravo [Psychology and law]. 2016. Tom 6. no. 4. pp. 86–94. doi:10.17759/psylaw.2016060409/ (In Russ., abstr. in Engl.).
23. Yurchenko O.P. Voprosy informatsionnoi bezopasnosti shkol'nikov v teorii i praktike sovremennogo frantsuzskogo mediaobrazovaniya [Information security in the context of the protection of children's rights in the Russian Federation]. Vestnik Chelyabinskogo gosudarstvennogo universiteta [Bulletin of Chelyabinsk State University]. 2013. no. 22 (313). Filologiya. Iskusstvovedenie. Vyp. 81. pp. 302–305.
24. O'Neill B., Staksrud E. Final recommendations for policy. London: EU Kids Online, LSE, 2014. p.42. URL: <http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20III/Reports/D64Policy.pdf>
25. Livingstone S., Cagiltay K., Ólafsson K. EU Kids Online II Dataset: A cross-national study of children's use of the Internet and its associated opportunities and risks/ British Journal of Educational Technology. Vol 46. No 5, 2015. pp. 988–992 doi:10.1111/bjet.12317