https://doi.org/10.32362/2500-316X-2019-7-4-21-30

УДК 621.311.6:621.3.089.2

Информационная безопасность ребенка в цифровом пространстве Российской Федерации

С.С. Дубов[@], В.В. Линьков, М.А. Карбаинова

Московский государственный университет геодезии и картографии, Москва 105064, Россия

[@]Автор для переписки, e-mail: Dubovss@gmail.com

В наше время стремительного развития социальных ресурсов интернет-технологий резко увеличивается количество пользователей всех возрастов, которые являются активными потребителями различного, в том числе и деструктивного, контента. Бурное развитие такого рода технологий порождает все новые и новые угрозы. Совершенствуются технологии информационных атак, направленных не только на программно-аппаратные платформы, но и непосредственно на пользователей информационных продуктов, распространяемых в среде Интернет. Изменяются инструменты информационного и психологического воздействия на пользователей Интернета. Различного рода мошенники и преступники в своей противоправной деятельности ищут и находят потенциальные «жертвы» в цифровой глобальной среде. Одной из самых уязвимых возрастных групп являются дети и подростки. Поэтому наиболее остро стоит вопрос о защите ребенка, «живущего» в такой среде. Настоящая статья посвящена проблеме обеспечения информационной безопасности детей и подростков в нашей стране в условиях формирования глобального информационного общества. Отражено основное противоречие существования и поведения ребенка в новом цифровом пространстве. Оно выражается в том, что, с одной стороны, виртуальная социальная активность ребенка – это залог его развития и процветания в будущем, а, с другой стороны, он подвергается рискам воздействия через неконтролируемые коммуникации и возможности открытого доступа к запрещенному контенту, которые в совокупности несут угрозы его психическому здоровью и благополучию. Сформулированы и проанализированы основные угрозы информационной безопасности ребенка в цифровом пространстве Российской Федерации. Даны предложения по созданию средств защиты подрастающего поколения от нового типа информационно-психологических угроз.

Ключевые слова: ИТ-образование, средства обеспечения информационной безопасности, социальная инженерия, взлом, аудит, уязвимости, защита.

Child's Information Security in Digital Space of the Russian Federation

Sergey S. Dubov[@],
Valeriy V. Linkov,
Mariya A. Karbainova

Moscow State University of Geodesy and Cartography, Moscow 105064, Russia
[@]Corresponding author e-mail: sDubovss@gmail.com

Our time is the time of rapid technological development. The Internet is becoming available to everyone, and it is expanding its influence in various fields. In addition, the number of users who are using the Internet and who are active consumers of different content is increasing. But the rapid development of technology has created new security problems. New types of threats are emerging, attack techniques are improving. Criminals are now trying to find their «victim»not only in the real world, but also in the digital world. So, today special attention is given to the issue of ensuring the user's information security and user's security in the digital world. One of the most vulnerable age groups are children. That is why one of the most important issues is the issue of protecting a child in such an environment. This article is devoted to the problem of information security of children and adolescents in our country. The article describes the main problem of the child in such an environment. On one hand, the virtual activity of the child is the key to its successful education. But, on the other hand, there are risks and problems in the digital world, such as access to prohibited content, that can cause harm to the mental health of a child. This article describes vulnerabilities in the information environment of students and educational institutions, as well as ways to counter the described vulnerabilities.

Keywords: IT education, information security tools, social engineering, hacking, auditing, vulnerabilities, protection, countering violations.

Хочешь победить врага, воспитай его детей.
Восточная мудрость

Введение

Во время формирования глобального информационного общества всеобщей компьютеризации и виртуализации, а также активного внедрения инструментов цифровой экономики во все аспекты жизни населения развитых стран как никогда остро встает вопрос обеспечения безопасности личных данных пользователей от компьютерных атак, а также самих пользователей от деструктивных информационно-психологических воздействий. По данным аналитического агентства WeAreSocial и крупнейшей SMM-платформы Hootsuite, представленном в отчетах о глобальном цифровом рынке GlobalDigital 2018[1], сегодня во всем мире Интернетом пользуются более 4 млрд человек. Одним из ключевых факторов роста интернет-аудитории стали доступные смартфоны и недорогие тарифы на мобильный Интернет. Теперь две трети из 7.6 млрд мирового населения имеют мобильные телефоны. Более половины из используемых сегодня мобильных устройств относятся к классу «умных», поэтому людям стано-

[1]https://www.web-canape.ru/business/internet-2017-2018-v-mire-i-v-rossii-snatistika-i-trendy/

вится все проще получить доступ ко всем возможностям, которые предлагает Интернет, где бы они не находились. Значительный рост происходит и в аудитории социальных сетей. За последние 12 месяцев количество людей на самых популярных социальных площадках увеличивалось ежедневно почти на 0.1 млн новых пользователей . Каждый месяц с соцсетями взаимодействуют более 3 млрд человек, при этом 9 из 10 – через мобильные устройства. По данным, приведенным в вышеуказанном отчете, почти половина (47%) населения России зарегистрирована в соцсетях и активно ими пользуется. 55.9 млн человек попадают туда с мобильных устройств. Среднестатистический россиянин проводит в соцсетях значительное количество времени – 2 часа 19 минут в сутки, а в Интернете – почти 6.5 часов в сутки. Стоит также отметить, что 85% россиян выходят в Интернет каждый день.

К сожалению, данные о процентном содержании возрастных групп в таком бурно растущем информационном обмене практически отсутствуют. Однако можно гарантированно утверждать, что подавляющее большинство школьников и подростковой молодежи имеют доступ к этим ресурсам и практически «живут» в глобальном виртуальном пространстве. К этому контингенту, не без участия родителей, активно подключаются и дети старших групп детсадовского возраста.

Механизмы глобальной визуализации, созданные маркетологами, графическими дизайнерами и визуальными инженерами в «умных» устройствах, позволяют снизить требования к квалификации своих пользователей настолько, что даже дети, еще не умеющие читать и писать, уже могут просматривать, передавать и даже размещать в Интернете фотографии и видеозаписи.

Масштабное профессиональное исследование вопросов, связанных с использованием Интернет-ресурсов детьми, было проведено компанией RUметрика[2]. Главными критериями анализа полученных данных, положенных в основу выводов, стали статистические показатели, виды доступа в Интернет (самостоятельно или под надзором родителей), а также анализ доступного материала, содержащего запрещенные элементы. В результате исследования сделаны некоторые выводы, в частности, статистика указывает на почти девятимиллионную детскую аудиторию Интернета, причем учтены только дети младше 14 лет, из которых три четверти пользуются Интернет-ресурсами без контроля со стороны родителей. Среди всей детской аудитории есть пользователи младше пяти лет, причем порядка 90% из них просматривают сайты под присмотром старших либо совместно с родителями; около 40% детей посещают сайты, где размещены порнографические материалы; примерно 20% детей просматривали в Интернете видео, содержащее сцены насилия и другие нежелательные материалы. Только половина детей не встречала в сети ссылок или ресурсов, содержание которых не предназначено для просмотра детям.

Защита детей и подростков от новых информационных угроз является неотъемлемой составляющей системы обеспечения информационной безопасности в Российской Федерации. Согласно действующей Доктрине информационной безопасности, принятой в России [1], под информационной безопасностью понимают 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

[2]https://studylib.ru/doc/866969/masshtabnoe-professional._noe-issledovanie-voprosov--svyazan...

и безопасность государства. Постулируя, что ребенок – это личность, член общества и гражданин, обладающий определенными правами и обязанностями (хотя и неполными до достижения возраста дееспособности), мы принимаем и интересы ребенка в информационной сфере как объект защиты. Кроме того, никто не станет спорить с истиной, что дети – наше будущее. Закладывая основы информационной безопасности на уровне информационных интересов детей, мы формируем стратегию информационной безопасности России [2].

Достижению этой важной задачи служит и подписанный совсем недавно Федеральный закон от 01.05.2019 № 93-ФЗ «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты Российской Федерации». Закон регулирует отношения, связанные с защитой детей от информации, причиняющей вред их здоровью и (или) развитию, в том числе от такой информации, содержащейся в информационной продукции.В Законе, в том числе, определен порядок реализации запрета на распространение среди детей информации, содержащей изображение или описание сексуального насилия[3].

Постановка проблемы

С приходом интернет-технологий в повседневную жизнь людей появились не только новые возможности, но и новые угрозы. С одной стороны, виртуальная социальная активность ребенка – это залог его развития и процветания в будущем, с другой стороны, появились риски использования им неконтролируемых коммуникаций и доступа к запрещенному контенту, которые угрожают его психическому здоровью и благополучию.

Обзор социальных уязвимостей школьника

Сегодня размещение информации о себе в сети не представляет никакой сложности:это можно сделать с компьютера, смартфона и других гаджетов, которые появляются у детей с раннего возраста. Однако дети они не всегда понимают, что можно, а что нельзя выкладывать в сеть, какие это несет последствия – в этом проблема. Уже сформировалось такое понятие, как цифровая репутация. Данное понятие применимо к юридическим и физическим лицам и отражает их деятельность в сети Интернет. Цифровая репутация играет важную роль в жизни человека. Корректно представленная позитивная информация дает преимущества и расширяет возможности. Благодаря грамотно созданному профилю в интернет-пространстве, можно достигнуть успеха в своей деятельности, найти единомышленников, партнеров, работодателей. Подростковая молодежь – особенно – находит таким образом возможность самовыражения через виртуальный мир, не находя понимания в мире реальном.

Многие пользователи используют социальные сети для передачи различной информации, в том числе, передают информацию, представляющую врачебную тайну, пароли, сведения о доходах и имуществе семьи, планируемых поездках и увлечениях. И такая информация, в зависимости от целей и намерений тех, кто получил к ней доступ, может быть использована по-разному. Стоит отметить факт того, что информация, попавшая в Интернет, остается там навсегда: «…копии информации делаются на множество серве-

[3]https://www.garant.ry/products/ipo/prime/doc72135250/

ров. История ваших действий – также пишется и протоколируется» [3].

Если человек намеренно оставляет информацию о себе в сети Интернет, то найти ее не сложно: для этого даже есть специальные программные сервисы, например, Яндекс. Люди, SocialMention и др. Во Всемирной паутине есть особые категории пользователей, которые собирают информацию о субъекте для совершения мошеннических действий. И чем больше данных о субъекте они смогут найти в интернет-пространстве, тем более широкий спектр мошеннических действий они смогут реализовать.

Подрастающему поколению важно понимать, что количество персональной информации о себе в интернет-пространстве стоит ограничить, чтобы не стать потенциальной жертвой злоумышленника. Возможностью для атаки могут послужить: фотографии дорогих приобретений, видео с близкими людьми, паспортные данные, адрес места жительства или регистрации, семейное положение, образование, сведения о доходах, номера мобильных телефонов друзей и родственников и т. п. Получив доступ к такого рода информации, злоумышленник может использовать ее не только против конкретного человека (ребенка), но и против его близких.

То, что происходит в сети, комментарии в адрес ребенка, подростка, так или иначе оказывают на него сильное социальное влияние, так как в школьном возрасте формируются сознание, мировоззрение, нравственные аспекты личности взрослого человека. В превалирующей степени это зависит от социальных составляющих, однако, не только от ближайшего окружения, но и глобального социально-культурного влияния.

Сейчас интернет-сервисы являются основным поставщиком информации, способом досуга. Важно понимать риски интернет-пространства: продолжительное пользование Интернетом несет вред физическому здоровью и психическому сознанию человека, особенно ребенка. Оно обусловлено контентом, который не предназначен для той или иной категории пользователей.

Вот несколько серьезных рисков злоупотребления пользования Интернетом:

- риск быть вовлеченным в секты, терроризм;
- доступ к материалам, повышающим риск подросткового суицида;
- искажение нравственных ценностей на основе увиденного контента;
- нанесение вреда физическому здоровью.

Действительно, в условиях формирования глобального информационного общества и, соответственно, создания сферы глобального информационного противоборства основными объектами интересов распространителей идеологии терроризма и экстремизма является массовое и индивидуальное сознание подростков и молодежи. Информационное воздействие осуществляется как на фоне информационного шума существующих и создаваемых технологий «BigData», так и в условиях информационного вакуума (внедрение измененных моральных ценностей). Совершенствуются практики внедрения психокомпьютерных технологий в социальные ресурсы Интернета с целью навязывания чуждых целей, вербовки адептов экстремистских идей, навязывания культа силы и безнаказанности. Побуждающей мотивацией инициаторов в качестве целеуказания при работе с массовыми молодежными аудиториями являются жажда власти и материального обогащения, а путями достижения целей – новые компьютерные технологии информационно-психологического воздействия на формирующиеся «малые миры», сообщества

юных пользователей социальных ресурсов по интересам.

Социальные сети – это еще один аспект Всемирной паутины, в которых присутствуют риски, связанные с общением, начиная от рекламы платных подписок до общения с посторонними, которые нередко присылают контент порнографического содержания или пропагандируют материалы, повышающие риск подросткового суицида. Массовую привязанность школьников к социальным сетям «ВКонтакте», «Facebook», «Одноклассники» можно объяснить наличием массы удобных сервисов так называемого «социального софта» [4]. Но отсутствие цензуры и безнаказанность зачастую приводят к неприятным, а порой и трагичным, инцидентам. Такие сети снабжены системами современной контекстной рекламы, с использованием которых можно без труда навязывать молодежи чуждые мысли и идеи и делать это максимально эффективно (распределение рекламы по целевым аудиториям: возраст, место жительства, учебы и др.). Крупные игроки рекламной сферы готовы раскрутить любую идею, не задумываясь о моральной составляющей [5]. Так, в рекламу внедряются не только порнография, но и пропаганда алкоголя, а также игры, провоцирующие насилие.

Запуская новые социально-ориентированные проекты в социальных ресурсах, которые интересны школьникам, инициаторы стремятся достичь максимального психологического воздействия на неустойчивую психику подростков, зачастую используя молодежный сленг, ненормативную лексику, скрытые и явные призывы к расизму, ксенофобии и национальной нетерпимости.

Когда ребенок погружается в общение в цифровом пространстве, то не задумывается о том, кто сидит по ту сторону экрана. При общении он использует ассоциативное мышление, что может быть крайне опасно. Большинство профессиональных мошенников и манипуляторов сознания обладают навыками социальной инженерии. Самый простой объект их «охоты» – ребенок, ведь к нему так просто войти в доверие. Существует множество случаев, в которых дети подвергаются социальному насилию. Грамотный социальный инженер может за небольшой промежуток времени довести ребенка до неуравновешенного состояния, после которого может произойти что-либо – от суицидов и преступлений до вымогательства, социальной изоляции не только в виртуальной, но и в реальной среде.

Закулисные специалисты и их публичные представители целенаправленно воспитывают российскую молодежь в деструктивном ключе. Они разрабатывают и реализуют «увлекательные» методики, специально рассчитанные их «педагогами» и «психологами» для незрелых умов и бурлящих чувств. Социотехнологии антигуманного характера оттачиваются на участниках молодежных «клубов самоубийц» в социальных сетях. Таким образом отрабатываются инструменты «расчеловечивания» молодого поколения, превращения его в слепое орудие чужой воли [6-9].

Невозможность контролировать виртуальные контакты ребенка

Если в реальной жизни мы можем запретить ребенку разговаривать с незнакомцами, то в виртуальной среде взрослый человек достаточно легко может замаскироваться. Регулирование круга общения ребенка в виртуальной среде для многих родителей является сложной, а порой и невыполнимой задачей, а если родители не следят за кругом общения

ребенка, он может не только попасть под плохое влияние, но и быть ввязан в политические дискуссии, завербован или психически сломлен.

Пока в образовании и в обществе в целом наблюдается «воспитательный вакуум», его заполняют весьма сомнительные, а зачастую и, несомненно, вредные «источники». Это «чернушные» кинофильмы, «рэп-культура», терпимость к «легким наркотикам», к половой неразборчивости, «европейская» мода на «унисекс». В компьютерном мире это социал-дарвинистские компьютерные игры-«стрелялки» и сектантские группы в социальных сетях. В качестве примера можно привести онлайн-игры. Ключевая опасность в них заключается именно в социальной части игр. В эти игры играют разные люди, из разных стран мира, в том числе и злоумышленники, и каждый из них может напрямую поговорить с ребенком.

Серьезную опасность для детей таит Даркнет (Darknet) – скрытая сеть интернет-соединений. Для одних – это зашифрованный мир скрытых сервисов Tor, в котором нельзя вычислить пользователей, для других – это те сайты, которые не индексируются обычными поисковыми системами: таинственные дебри запароленных веб-ресурсов, не связанных друг с другом страниц и скрытого контента, доступного только «своим», для кого-то – это просто общее понятие, под которым подразумевается вся та бездна шокирующих, пугающих и провокационных уголков Интернета, где обитают воображаемые преступники и злодеи всех мастей и калибров. Гораздо важнее суть данного явления: это не просто подполье, изолированное от привычного нам Интернета, и при том все же являющееся его частью, царством полной свободы и анонимности, где пользователи говорят и думают то, что им нравится, без цензуры, без правил, без общественных рамок. Эта реальность, столь же шокирующая и пугающая, сколь и прогрессивная, и творческая, и она гораздо ближе к нам, чем мы думаем.

Даркнет редко сходит с новостных заголовков – молодые люди выкладывают любительскую порнографию, кибербуллеры (люди, насмешками и угрозами пугающие или унижающие человека) и тролли досаждают незнакомым людям, политические экстремисты занимаются пропагандой, контрабанда, наркотики и секретные документы можно купить в один-два клика – все эти рассказы каждый день мелькают на первых полосах. Но как ни странно, этот мир практически не изведан и непонятен большинству из нас. Немногие решались погрузиться в глубины Интернета и хоть одним глазком поглядеть на эти сайты [10].

Эта неизвестность сильно привлекает подростков, но из-за чересчур открытого информационного пространства и весьма простого доступа к любым данным, все найденное в Даркнете становится свободно от норм и правил. Это большая опасность даже для взрослого человека, а для подростка данная доступность может оказаться критической. Подростковая психика может не выдержать порцию очередного контента, подросток может потерять связь с реальностью и, сам того не подозревая, стать оружием в руках профессиональных вербовщиков Даркнета [11].

В связи с геометрическим ростом количества пользователей, их потребностей и возможностей в цифровом пространстве появилась потребность и в их защите.

Защита ребенка в цифровом пространстве

Детские психологи выделяют главный метод защиты ребенка от социальных угроз – общение с ребенком. Общаться с ребенком нужно все время, причем и в реальном, и в

виртуальном пространстве. Необходимо стать не только его родителем, но и его старшим другом, который сможет не только объяснить ребенку, что ему делать, но и понять его психологию и, следовательно, его слабости. Только родитель сможет оградить ребенка от опасности как в реальной, так и в виртуальной жизни. Однако в настоящее время многие родители не имеют навыков для обеспечения контроля поведения ребенка в цифровом пространстве.

В связи с этим предлагается создать инструмент, позволяющий контролировать социальную активность ребенка, размещаемую и просматриваемую им информацию в сети Интернет. Этот инструмент может быть построен по принципу DLP-систем: учитывать частоту, время использования гаджета, анализировать содержание просматриваемого контента, идентифицировать контакты, просматривать входящие и исходящие SMS, отслеживать интернет-трафик, геолокацию телефона и др. Архитектура такого инструмента должна быть построена на модели клиент–сервер (клиент – это гаджет ребенка, сервер – это гаджет родителя). Инструмент должен иметь возможность установки на любую платформу и отвечать системным требованиям устройств родителей и детей. У родителей должен быть способ изменять и дополнять базы данных с разрешенным и запрещенным контентом, опираясь на статистику активности ребенка, будь то игры, чаты, звонки, время использования гаджета на различных ресурсах и т. д. Оповещение и контроль над действиями ребенка могут осуществляться как через SMS-оповещения, так и через онлайн-мониторинг в приложении. SMS-оповещения могут быть полезны для своевременного реагирования, когда устройство родителя находится в офлайн-режиме.

Подобный инструмент контроля должен быть скрыт от ребенка, так как в большинстве случаев дети негативно реагируют на запреты и ограничения. Этот инструмент позволит, кроме того, родителям, страдающим цифровой безграмотностью, «не упустить» ребенка, защитить его и помогать активно развиваться в слабо доступной для родителей среде , проводя комплексный воспитательный процесс. Ведь «лучший способ защиты детей – правильное воспитание» [12] .

Выводы

Негативные информационные воздействия для современных школьников, осуществляемые посредством доступных интернет-сервисов и мобильных платформ, к сожалению, начинают играют роль основного воспитателя. Разрабатываемая система мониторинга социальной активности ребенка, размещаемой и просматриваемой им информации в сети Интернет должна укрепить связь с родителями, защитить учащихся от негативных информационно-психологических воздействий и противодействовать им.

Литература:

1. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента Российской Федерации от 5 декабря 2016 г. № 646. URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html (дата обращения: 15.06.2019).

2. Шпагина Е.М. Информационная безопасность в контексте защиты прав детей в Российской Федерации [Электронный ресурс] // Психология и право. 2016. Т. 6. № 4. С. 86–94. https://doi.org/10.17759/psylaw.2016060409

3. Ли П. Архитектура интернета вещей: пер. с англ. М.: ДМК Пресс, 2018. 456 с. ISBN: 978-5-97060-672-8.

4. Грингард С. Интернет вещей. Будущее уже здесь. М.: Альпина Паблишер, 2016. 188 с.

5. Маркелов А. Openstack. Практическое знакомство с облачной операционной системой. М.: ДМК Пресс, 2018. 306 с. ISBN 978-5-97060-652-0.

6. Посыпкина Александра, Баленко Евгения. Профиль в цифрах: как будет работать база данных о россиянах в 2023 году. 2018 г. [Электронный ресурс] – https://www.rbc.ru/technology_and_media/20/09/2018/5ba262ef9a7947c2ab193522 (дата обращения: 17.06.2019).

7. Хапаев Дмитрий. Как узнать, какие данные собирает о вас гугл… 2018 г. [Электронный ресурс] – https://lifehacker.ru/slezhka-google/ (дата обращения 15.06.2019).

8. Защита детей от вредной информации в сети интернет [Электронный ресурс] – http://www.internet-kontrol.ru/ (дата обращения: 10.06.2019).

9. Чернова Ирина. 15 фишек для сбора информации о человеке в интернете. 2016 г. [Электронный ресурс] – https://www.iphones.ru/iNotes/533552 (дата обращения: 15.06.2019).

10. Бартлетт Д. Подпольный Интернет. Тёмная сторона мировой паутины. Civilизация: пер. с англ. М.: Изд-во ЭКСМО, 2017. 352 с. ISBN: 978-5-699-85457-8.

11. Идальго С. Как информация управляет миром и определяет историю нашей вселенной и живущих в ней видов: Civilизация: пер. с англ. М.: Изд-во ЭКСМО, 2016. 256 с. ISBN: 978-5-699-85453-0.

12. Игнатова Наталья. Ваш цифровой портрет в сети. 2015 г. [Электронный ресурс] – https://geekbrains.ru/posts/digital_portrait (дата обращения: 11.06.2019).

References:

1. Doctrine of Information Security of the Russian Federation (App. Decree of the President of the Russian Federation, December 5, 2016, no. 646) URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html. Accessed June 15, 2019 (in Russ.).

2. Shpagina E.M. Information security in the context of the protection of children's rights in the Russian Federation [Electronic resource]. *Psikhologiia i pravo* [Psychology and Law], 2016; 6(4):86-94. http://dx.doi.org/10.17759/psylaw.2016060409 (in Russ.).

3. Lea P. Internet of Things for Architects. Packt Publishing, 2018.

4. Greengard S. The Internet of Things. Moscow: Alpina Publisher, 2016. 188 p., (in Russ.).

5. Markelov A. Openstack. Practical familiarity with the cloud operating system. Moscow: DMK Press Publ., 2018. 306 p., (in Russ.).

6. Posypkina A., Balenko E. Profile in Figures: How the Database of Russians Will Work in 2023. 2018. URL: https://www.rbc.ru/technology_and_media/20/09/2018/5ba262ef9a7947c2ab193522. Accessed June 17, 2019 (in Russ.).

7. Khapaev D. How to Find out What Data Google Collects about You… 2018. URL: https://lifehacker.ru/slezhka-google/. Accessed June 15, 2019 (in Russ.).

8. Children' Protection from Harmful Information in the Internet. URL: http://www.internet-kontrol.ru/. Accessed June 10, 2019 (in Russ.).

9. Chernova I. 15 Pieces to Collect Information about a Person in the Internet. 2016. URL: https://www.iphones.ru/iNotes/533552. Accessed June 15, 2019 (in Russ.).

10. Bartlett D. The Dark Net: Inside the Digital Underworld. London: Melville House Publishing, 2015. 310 p. ISBN: 978-1-61219-489-9.

11. Hidalgo C. Why Information Grows: The Evolution of Order from Atoms to Economies. New York: Basic Books, 2015. ISBN 978-0465048991

12. Ignatova N. Your Digital Portrait Online. 2015. URL: https://geekbrains.ru/posts/digital_portrait. Accessed June 11, 2019 (in Russ.).

Об авторах:

Дубов Сергей Сергеевич, кандидат технических наук, директор центра отраслевых мониторинговых систем и информационной безопасности, доцент кафедры информационно-измерительных систем Московского государственного университета геодезии и картографии (МИИГАиК) (Россия, 105064, Москва, Гороховский пер., д. 4).

Линьков Валерий Владимирович, студент Московского государственного университета геодезии и картографии (МИИГАиК), сетевой инженер Cisco по направлениям CCNA, CCNA Security, CCNA Cyber Ops, Инструктор сетевой академии Cisco «Learning Resource Center «Ramix» (Россия, 105064, Москва, Гороховский пер., д. 4).

Карбаинова Мария Александровна, студент Московского государственного университета геодезии и картографии (МИИГАиК) (Россия, 105064, Москва, Гороховский пер., д. 4).

About the authors:

Sergei S. Dubov, Cand. of Sci. (Engineering), Director of the Center for Sectoral Monitoring Systems and Information Security, Associate Professor, Chair of Information and Measuring Systems, Moscow State University of Geodesy and Cartography (MIIGAiK) (4, Gorokhovskii per., Moscow, 105064, Russia). E-mail: Dubovss@gmail.com.

Valeriy V. Linkov, Student of Moscow State University of Geodesy and Cartography (MIIGAiK), Network Cisco Engineer in CCNA, CCNA Security, CCNA Cyber Ops, Instructor of Cisco Academy «Learning Resources Center «Ramix» (4, Gorokhovskii per., Moscow, 105064, Russia).

Mariya M. Karbainova, Student of Moscow State University of Geodesy and Cartography (MIIGAiK) (4, Gorokhovskii per., Moscow, 105064, Russia).

Для цитирования: Дубов С.С., Линьков В.В., Карбаинова М.А. Информационная безопасность ребенка в цифровом пространстве Российской Федерации // Российский технологический журнал. 2019. Т. 7. № 4. С. 21–30. https://doi.org/10.32362/2500-316X-2019-7-4-21-30

For citation: Dubov S.S., Linkov V.V., Karbainova M.A. Child's information security in digital space of the Russian Federation. *Rossiiskii tekhnologicheskii zhurnal* = Russian Technological Journal. 2019; 7(4):21-30, (in Russ.). https://doi.org/10.32362/2500-316X-2019-7-4-21-30