АКТУАЛЬНЫЕ ТЕНДЕНЦИИ СОЦИАЛЬНЫХ КОММУНИКАЦИЙ

ИСТОРИЯ И СОВРЕМЕННОСТЬ

Сборник научных статей

Current Trends of Social Communications:
History and Contemporaneity
Collected articles

Ижевск
2017

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФГБОУ ВО «УДМУРТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ИНСТИТУТ СОЦИАЛЬНЫХ КОММУНИКАЦИЙ

The Russian Federation Ministry of Education and Science
Federal State Budgetary Educational Institution of Higher Education
"Udmurt State University"
Institute of Social Communications

АКТУАЛЬНЫЕ ТЕНДЕНЦИИ СОЦИАЛЬНЫХ КОММУНИКАЦИЙ: ИСТОРИЯ И СОВРЕМЕННОСТЬ

Сборник научных статей

Current Trends of Social Communications:
History and Contemporaneity
Collected articles

ИЖЕВСК
Izhevsk
2017

УДК 3:001.12
ББК 60я43
А 437

Журнал включен
в реферативную базу РИНЦ

Научный редактор:
доктор исторических наук, профессор Г.В. Мерзлякова.

А 437 Актуальные тенденции социальных коммуникаций: история и современность. Сборник научных статей. (Материалы Международной научно-практической конференции «Актуальные тенденции социальных коммуникаций: история и современность», 30 октября 2017 г., Ижевск) / Под. ред. Г. В. Мерзляковой, Л. В. Баталовой, С. А. Даньшиной, Н. А. Кононовой, Е. И. Михалёвой – Ижевск: Издательский центр «Удмуртский университет», 2017. – 320 с.

ISBN 978-5-4312-0535-4

В сборнике представлены статьи посвященные исследованиям социально-коммуникативных процессов, развитию медиакоммуникаций, изучению инновационных возможностей регионального туризма.

Данный сборник предназначен для исследователей в области гуманитарных наук, а также для специалистов, интересующихся различными аспектами практической деятельности и современными технологиями в области интернет-пространства, организации деятельности в области рекламы, связей с общественностью, туризма и молодежной политики. Материалы сборника могут быть использованы студентами, магистрантами и преподавателями в учебном процессе.

В сборнике представлены статьи ученых и преподавателей из г. Кирова, Москвы, Нью - Йорка, Парижа, Томска, Ярославля и др.

УДК 3:001.12
ББК 60я43
А 437

ISBN 978-5-4312-0535-4

СОДЕРЖАНИЕ

УДК (045)

Фефилов Антон Валерьевич
Кандидат психологических наук, доцент,
доцент кафедры общей психологии,
зав. лабораторией психофизиологии и
экспериментальной психологии ИППСТ
ФГБОУ ВО «УдГУ».
Россия, г. Ижевск.
antfefilov@yandex.ru, fefilov@udm.ru

Fefilov Anton V.
Udmurt State University
Russia, Izhevsk.

КУЛЬТУРА И БЕЗОПАСНОСТЬ В СОВРЕМЕННОМ ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ И ОСНОВНЫЕ АКТУАЛЬНЫЕ УГРОЗЫ ДЛЯ НИХ

CULTURE AND SAFETY IN THE MODERN INFOMATIONAL SPACE AND THE MAIN ACTUAL THREATS FOR THEM.

Аннотация

Статья описывает разные аспекты культуры и норм общения и работы в интернете, особенно в социальных сетях, причины агрессии и интернет-троллинга. Акцентируется внимание на вопросах влияния искусственного интеллекта и компьютеров вообще на жизнь и работу людей, опасности замены компьютерами отдельных психических функций и целых индивидов.

В статье обсуждаются проблемы защиты и сохранения конфиденциальности личной информации, опасности уничтожения информации и несанкционированного доступа к данным. Анализируются современные и более явные информационные угрозы, включая различные вирусы, атаки компьютера хакерами, недостаточные знания и опыт работы самих пользователей, в том числе системных администраторов и программистов.

Описываются различные виды защиты от вирусов, включая специальные программы и патчи против вирусов типа Ванна-Край, которые выпускаются в Майкрософт и других международных компаниях. В статье сравниваются подходы разных фирм-создателей программного обеспечения к работе на интернет-сайтах вообще и с личной конфиденциальной информацией особенно. Обсуждаются стратегии защиты компьютеров и смартфонов международных компаний Гугл, Эппл и Майкрософт.

Ключевые слова: культура интернет-коммуникации, источники агрессии, интернет- троллинг, ИТ-технологии, компьютеры, искусственный интеллект, информационная безопасность, вирус и антивирусы.

Abstract

The article describes the different aspects of the internet communication and working' culture and standard, especially in social network, sources of aggression and internet-trolling. It makes accent on (about) artificial intellect and computer's influence on the people's life and working, danger of computer substitution of the separate psychic functions and individuals.

In the article it discusses the personal information confidentiality's safety and preservation' problems,

danger of the information destruction and unauthorized data access. It is analyzing actual and more obvious informational threats, including different viruses, hacker's computer attacks, user's known and experience's deficit, e.g. in system administrators and programmers.

The article describes different kinds of the modern antivirus safety and defense, including special programs and patches for WannaCry-type viruses, which are produced by Microsoft and other international companies. In the article it compares the different companies-creators of the computer programs' approaches to the work on internet sites generally and with the personal confidential information especially. It discusses the computer and smartphone's safety and defense strategies of the Google, Apple and Microsoft international companies.

Keywords: Culture of the internet communication, sources of aggression, internet-trolling, IT-technologies, computers, artificial intellect, information's safety, virus and antiviruses.

Очень быстрое развитие ИТ-технологий и в том числе сферы интернет-коммуникации в мире и в России породило как множество новых возможностей, так и массу новых проблем. Социальные сети, форумы, блоги, другие ресурсы стали лакмусовой бумажкой для проявления уровня социального, культурного, морально-психологического, интеллектуального и других сфер развития всех субъектов, участвующих в процессе коммуникации [1, С. 255-260; 2, С. 69-73].

«Комментарии, наполненные ненавистью, стали достаточно серьезной проблемой всех социальных сетей, но в России пока нет какой-либо законодательной базы, позволяющей привлечь злопыхателей к ответственности. Тем не менее каждый психолог понимает, что от такого рода посланий исходит «существенная угроза общественному спокойствию». В Европе сетевой беспредел уже заметили на политическом уровне. Власти открыто предупреждают, что если сами сети – Facebook, Google, Twitter не справятся с этой проблемой, то придется вмешаться Евросоюзу [10, С. 22, 22-24].

Почему же внезапно возникла эта массовая тенденция к вызывающему поведению, почему люди проявляют такую вербальную агрессию в отношении других людей», чем-то отличающихся от них самих? Возникает также вопрос, «ведут ли люди себя при цифровой коммуникации иначе, чем в реальной жизни, и почему»? Социолог, доктор, профессор Армин Нассеи постоянно говорит о том, что приводит к появлению разного рода «постов ненависти» в интернете и почему порог сдерживания во Всемирной сети гораздо ниже, нежели в обычной (привычной) жизни. «В Интернете люди практически ничем не рискуют, - замечает социолог, - Поэтому другой становится и коммуникация. Те естественные ограничители, которые есть у нас при общении лицом к лицу, там отсутствуют» [10, С. 22-24].

Нассеи также считает, что «люди обретают уверенность в себе, если они замечают, что другие, даже абсолютно чужие люди, разделяют их мнение. И где это выражено так же ярко, как не в Интернете?» Европейский специалист по конфликтологии профессор Ульрих Вагнер добавляет: «В Сети зачастую утрачивается механизм самоконтроля. Там люди позволяют себе такие высказывания, которых они никогда бы не допустили в личном общении». В качестве причины он называет анонимность, которой пользуются многие пользователи, а также сопутствующие обстоятельства. «Многие обсуждения начинаются по ночам, когда люди, возможно, находятся под воздействием алкоголя и в одиночестве сидят перед монитором. И при этом

легко срабатывает спусковой механизм» [10, С. 22-24].

«Провоцируют конфликт и приходят в ярость в обсуждениях в Сети чаще всего те люди, которые и в реальной жизни отличаются особой импульсивностью и быстрой возбудимостью. «Дело в том, что многие дискуссионные форумы становятся поляризованными», - считает Вагнер. Многие люди, имеющие общее мнение, выступают также сообща и взаимно подпитывают друг друга. Собственно, тоже ничего экстраординарного, ведь мы охотнее общаемся с людьми, которые думают так же, как мы, разделяют наши мнения и которых волнуют те же вещи, что и нас» [10, С. 22-24].

«Опасным это становится тогда, когда появляются призывы к действиям за пределами Интернета», - говорит Ульрих Вагнер, давая пищу для размышлений. Ощущая поддержку людей с одинаковым мнением, можно стать неким мстителем. И все это под девизом: «другие думают как я, и теперь я возьму в свои руки то, что другие не осмеливаются» [10, С. 22-24].

Часть причин опасной переоценки пользователем Интернета и соцсетей своих прав и возможностей, знаний и умений, компетентности в разных вопросах кроется в особом влиянии на человеческий мозг вычислительной техники [3, С. 64-68]. Она эффективно подменяет или усиливает некоторые человеческие способности, связанные с памятью, восприятием, мышлением и даже творческими процессами, уменьшая нагрузку на сами мозг и психику и приводя их к постепенной деградации или остановке роста.

«Если мы слишком часто полагаемся исключительно на компьютер (смартфон, планшет) и меньше информации сохраняем в собственной памяти, мы в целом можем запоминать меньше. В этой связи Манфред Шпитцер говорит о «цифровом слабоумии». В его одноименном бестеллере, который вызвал дискуссии во всем мире, приведены примеры последствий чрезмерного использования цифровых устройств в молодые годы. Итоговый вывод такой: из-за интенсивного использования этих средств человеческий мозг деградирует, и, в частности, дети и подростки оказываются практически неспособными к обучению. Значит ли это, что компьютеры лишают нас ума?» [9, С. 16-18].

«Одно очевидно: мы своими руками создаем у себя зависимость от компьютеров. И хотя они еще не в полной мере освоили нашу деятельность, они влияют на нее и зачастую вносят глубокие изменения. А одновременно с этим меняются и наши способности. К примеру, специалисты по авиации выяснили, что из-за автоматизации (управления самолетом) многие пилоты совершенно разучились самостоятельно реагировать на определенные события и ситуации. То же самое касается и врачей, которые при постановке диагноза или во время операций полагаются в первую очередь на компьютерные системы. Здесь эксперты также обнаружили, что из-за возросшего использования компьютеров у медиков может развиться «туннельное» видение, мешающее формированию собственных интерпретаций и диагнозов. Наши знания очень часто тоже хранятся в электронном виде [9, С. 16-18].

«Томас Метцингер выходит далеко за рамки философии духа, на которой он специализируется. Философ исследует человеческое сознание и очень интенсивно занимается вопросами искусственного интеллекта. Его критика в отношении трансгуманизма никоим

образом не должна пониматься как картбланш для игнорирования технологической сингулярности интеллектуального взрыва [8, С. 22-26].

На вопрос, стоит ли нам опасаться супер-разума, Метцингер отвечает «Да, поскольку неясно, какие предпочтения и цели будут у такого искусственного интеллекта. Но страх никогда не был хорошим советчиком, и мы должны подходить к ситуации рационально и на основе очевидных фактов. Я бы сравнил ее с концентрацией всей финансовой власти в руках богатейшего одного процента населения планеты». По его словам, существует немалый риск, что нечто подобное произойдет и с «когнитивной властью», но при этом она будет сконцентрирована вне человечества [8, С. 22-26].

Базирующийся в Швейцарии «Институт эффективного альтруизма» также занимается этим вопросом: «Супер-разум по определению не может быть глупым: если существует опасность, что вы вытащите вилку из розетки, то сначала он будет вести себя так, как желает создатель, пока не найдет способа минимизировать принудительную деактивацию». Институт опубликовал доступный для обсуждения доклад с рекомендациями относительно возможностей и рисков искусственного интеллекта. Предложения института следует также понимать как призыв к тому, чтобы придать теме искусственного интеллекта глобальный приоритет. К примеру, требуется больше грантов для исследователей для проведения анализа и предупреждения усугубления проблемы. Политики должны выделять больше ресурсов для научно-этического сопровождения технологических разработок. В предотвращении технологической гонки вооружений должно помочь и усиленное международное сотрудничество» [8, С. 22-26].

«Ситуация несколько напоминает разработку ядерного оружия. Каждый ученый, который участвовал в проекте «Манхэттен», знал, насколько опасна атомная взрывная мощь, но исследования не останавливались. Всегда были причины продолжать – от ситуации в большой политике до собственной меркантильности» [8, С. 22-26].

Помимо более абстрактных пока опасностей и вызовов для всего человечества компьютеризация и автоматизация представляют и другие, уже намного более близкие и явные для нас угрозы – например, в сфере занятости, где машины все больше вытесняют людей из производственных процессов и все чаще лишают нас работы.

Еще более актуальной и принципиально опасной для нас проблемой является резко нарастающее и уже массовое использование нами разнообразных электронных устройств и Интернета. Тесно связанной с почти всеми предыдущими проблемными вопросами является опасность нарушения конфиденциальности и защиты личной и общественной информации, а иногда и использование ее во вред самим людям.

С одной стороны, резкое повышение частоты обращения и отдельными людьми и организациями в целом за помощью в работе к компьютерам, смартфонам, цифровому телевидению, интернет-банкам, другим сайтам, электронным почтам и социальным сетям повышает вероятность заражения технических устройств различными вирусами и другими средствами, нарушающими затем и конфиденциальность и сохранность личных

данных [2, С. 69-73; 4; 5, С. 42-46; 6, С. 40-42; 11, С. 52-59].

С другой, возникающее расслоение пользователей компьютеров, сетей и смартфонов как минимум по уровню компетентности в сфере ИТ вообще и защиты информации в частности, приводит к усилению чувства безнаказанности тех, кто использует чужую информацию без ведома и часто во вред ее владельцам, и часто провоцирует больше еще негативных эмоций в сети, включая агрессию, тревогу, разные страхи и переживания потери чего-то важного.

Первые весьма серьезные и разрушительные «эпидемии» компьютерных вирусов, написанных для Windows 95, прошли во второй половине 1990-х гг. Так, «эпидемия вируса Win95.CIH, также известного как «Чернобыль» и поразившего компьютеры впервые 26 апреля 1999 года, была на то время самой разрушительной. Этот вирус активизировался 26 апреля и уничтожал информацию на жестких дисках, записывая на них случайный мусор. Кроме того, он перезаписывал Flash BIOS, если переключатель давал разрешение на запись, и выводил из строя материнскую плату компьютера» [4, С. 13-14].

«Червь» «I Love You», выпущенный на Филиппинах в мае 2000 года, нанес владельцам компьютеров ущерб на сумму, превышающую 10 миллиардов долларов. Обычно авторами вирусов являются профессионалы – программисты, знающие хотя бы один из языков программирования. Но по мере совершенствования ИТ-технологий вирусы писать все проще, и уже в 2001 году «автором «червя», под названием «Anna Kournikova», оказался голландский студент, который вообще не умел программировать, даже на таком простом языке, как Basic [4, С. 13-14].

В июне 2004 года был обнаружен первый «мобильный» червь – Cabir (созданный для мобильных телефонов). В марте 2005 года появился первый «червь», способный размножаться посредством MMS [4, С. 13-14].

В последние годы и месяцы количество и, главное, уровень опасности информационных заражений и взломов по всему миру резко возросли. В период с весны по лето 2017 г. произошли 3-4 события, которые показали, что без качественных изменений в сфере информационной безопасности и экономика стран в целом, как и стабильная работа отдельных компаний и заводов, в том числе школ, университетов, научных институтов и академий, банков, больниц, телекоммуникационных сетей, интернет-провайдеров и даже отдельных подразделений и государственных органов, включая МВД и Вооруженные силы, в разных странах будет оставаться в сложной и непредсказуемой ситуации.

Это показали и события середины мая 2017 г., когда внезапно в мире появился вирус WannaCry который атаковал, зашифровывал и затем уничтожал файлы на компьютерах с ОС Microsoft Windows, где отсутствовали регулярные критические и важные обновления, особенно от марта – апреля 2017г. Причем после попадания в локальные корпоративные и домашние сети скорость его распространения резко возрастала [12, 13, 16].

Летом появился схожий вирус Petya, жертвами которого стали снова очень многие компании и частные лица мира, но уже не только в России, а в большей степени на Украине и СНГ. Хотя и крупные компании РФ также попали под удар - прежде всего такие нефтегиганты, как «Роснефть» и «Башнефть» [14, 15], (так-

же как и ранее еще в мае – некоторые мобильные операторы РФ).

Около 20 июля 2017 появилась информация, что американские эксперты по информационной защите создали программу, которая направляет фрагменты вирусов на устройства под управлением Google Android и тестирует ими защитные программы, которые там установлены, на предмет поиска уязвимостей в антивирусах. Таким образом, эта программа смогла обойти около 50 антивирусных программ, включая все известные в мире и России бренды [17]. В следующий раз авторы программы обещали создать ее аналог для поиска обходов антивирусов для обычных компьютеров с ОС Microsoft Windows.

Тем временем количество мобильных и домашних устройств, которые регулярно выходят в интернет, превысило число стационарных компьютеров и ноутбуков. Это значит, что в области безопасности на первый план выходят задачи и методы защиты корпоративных и частных сетей и устройств под управлением ОС Google Android (большинство - на смартфонах, планшетах, телевизорах), а также Apple iOS.

Тем не менее, в перспективе защита самой ОС Microsoft Windows, которая пока еще является основной ОС для ПК и ноутбуков (особенно для работы в плане обработки и хранения больших массивов промышленных, финансовых и научных данных) и также очень нерегулярно обновляется на многих устройствах, особенно в смысле защиты, с одной стороны, все еще остается весьма актуальной, с другой - постепенно отходит на второй план.

Очень многие из упущений в информационной защите происходят в большой степени по чисто психологическим причинам, как со стороны простых пользователей, так и со стороны инженеров компаний и банков, и даже программистов самих разработчиков программного обеспечения! Например, обычные пользователи и сисадмины, как даже специалисты по информационной безопасности, могут быть излишне уверены в надежности защиты своих устройств, паролей к учетным записям и самих локальных сетей и вследствие этого, допускают серьезные ошибки в работе с информацией.

Также это может быть следствием особых черт характера, темперамента, излишней стрессоустойчивости, имеющегося опыта и образования, да и просто банального снижения психофизического состояния и усталости работников, включая и сисадминов. В этом вопросе может помочь психология и психофизиология, имеющая на вооружении различные методы оценки индивидуальных свойств характера и темперамента, а также эмоциональных и других состояний людей.

Конечно, различные политики централизованной корпоративной безопасности создаются с целью снизить зависимость вероятности заражения ИТ-систем от человеческого фактора, включая и психические состояния и мотивацию ИТ-работников и их клиентов. Они усложняют возможности заражения устройств компаний непосредственно из интернета, но часто облегчают при этом последующее распространение вирусов по локальным сетям. Если как обычно, применяются политики безопасности сетей «по умолчанию» (и в настройках учетных записей в ОС компьютеров, и у браузеров, и брандмауэров-файерволов, и у самих корпоративных антивирусных программ).

Следует учесть, что на большинстве

предприятий, госучреждений и ряде банков многие обновления защитных программ и самих ОС, включая антивирусные, осуществляются централизованно, с помощью одного или нескольких компьютеров и локальных сетей, видимо, в целях контроля и экономии большого программного интернет-трафика. Поэтому в настоящее время это может значительно увеличить риски взлома корпоративных сетей. Достаточно всего лишь либо заразить один (два-три) компьютера или сервера, которые принимают обновления баз от антивирусной компании, а также от серверов других поставщиков программ, (и /или просто даже роутеры, коммутаторы, смартфоны и модемы, через которые также могут идти эти важные обновления безопасности программ и баз, в том числе с помощью файлов на флешках, дисках и других устройствах), и тогда все остальные компьютеры, модемы и роутеры в локальных сетях предприятия также будут вначале исследованы на предмет заражения, а затем и реально заражены.

Иногда в компаниях и у частных лиц не обновляются регулярно не только ОС и встроенные программы Microsoft, но и сторонние интернет-браузеры, различные программы, драйверы и другие продукты - от компаний Adobe и Oracle Java (которые чаще всех являются источниками «дыр» и уязвимостей), а также Mozilla, Opera, Google, HP, LG, Toshiba, Samsung и прочие.

Что же касается самих фирм, контролирующих безопасность своих продуктов, то «при этом надо иметь в виду, что Google не так внимательно относится к вопросам обеспечения информационной безопасности мобильных устройств, как другие известные производители операционных систем – Microsoft и Apple (iOS) [7, С. 68-73]. В 59 % от всех «устройств на базе Android зияет огромная прореха в безопасности. Эта уязвимость позволяет хакерам, помимо прочего, просматривать электронную почту и даже удаленно управлять мобильными телефонами. Данная проблема касается нескольких сотен миллионов пользователей. Ужасает другое: все они брошены концерном Google и большинством производителей гаджетов на произвол судьбы [7, С. 68-71].

Эту уязвимость, касающуюся примерно 60 % всех активных устройств с Android (по данным на середину 2015 г.), можно разрешить или устранить, однако содействия от Google ждать не приходится. Концерн аргументирует это тем, что в версиях 4.4 и 5.0 проблема эта решена, таким образом считая, что долг выполнен. Однако многие не самые современные аппараты не получают обновление на такие версии. Поэтому их владельцам необходимо взять ситуацию в свои руки» [7, С. 68-71].

Уязвимости «скрываются» и в Apple iOS. «Поскольку Apple проверяет программные продукты гораздо строже, чем Google, прежде чем сделать их доступными в соответствующем сервисе, для устройств iPhone и iPad вредоносных программ практически нет. Однако даже iOS не безгрешна: вместе с обновлением на версию 8.3 (2015 года) компания опубликовала список почти из 60 уязвимостей, которые были устранены в новом варианте операционной системы…» [7, С. 72-73].

«Подход Apple к выпуску обновлений иной, нежели у партнеров Google: они разрабатываются практически для всех устройств, даже для морально устаревших. Версия iOS 8.3 работает на всех моделях iPhone вплоть до вышедшей еще несколько лет назад 4s».

Тем не менее, 22 % активных устройств от Apple не получат это обновление, поэтому не смогут быть хорошо защищенными» [7, С. 72-73].

Что же касается мобильной продукции Microsoft, то она «контролирует приложения даже строже компании Apple», - поясняет эксперт в области компьютерной безопасности компании AV-Test Майк Моргенштерн. «Даже если кто-то получит доступ к приложению, он еще долго не сможет взломать систему», - утверждает Моргенштерн. Поскольку Microsoft регулярно снабжает свои мобильные устройства (как и обычные компьютеры) обновлениями, Windows Phone – отличный выбор для пользователей смартфонов, обеспокоенных своей безопасностью [7, С. 72-73].

Microsoft предъявляет повышенные требования к аппаратному и программному обеспечению смартфонов. Кроме того, данная мобильная ОС обладает продвинутыми встроенными механизмами безопасности. Все это делает устройства на Windows Phone 8 и 8.1. одними из самых взломостойких в мире, что подтверждено наличием у них различных сертификатов» [7, С. 68-73].

Как бы то ни было, для обеспечения максимальной конфиденциальности, безопасности и культуры работы в интернете требуются и различные способности, и и свойства характера и темперамента, и знания, и опыт, и многое другое. У большинства сотрудников лаборатории психофизиологии и экспериментальной психологии ИППСТ УдГУ есть многое из перечисленного, а также и хорошо наработанные схемы оценки и нужных психических свойств и состояний работников. В разной степени подходящих или опасных для работы в интернете и просто с важной информацией. Также имеются и специальные средства и методы помощи в указанных вопросах, и даже алгоритмы вычисления и прогноза вероятности достижений или ошибок работников в разные периоды времени.

Мы также владеем определенными компетенциями защищенной работы на компьютерах и в разных сетях и сайтах, и на основе этого можем осуществлять консультации по вопросам ИТ. В том числе и в области сохранения психологического здоровья и психического состояния при работе с информацией, и самой комплексной защиты устройств и надежного хранения информации на компьютерах, смартфонах, планшетах [2, С. 69-73].

СПИСОК ЛИТЕРАТУРЫ

1. Фефилов А.В. Высшее образование в мире в России, плюсы и минусы от реализации его дистанционных форм в связи с количеством пользователей Интернет-сети, активных сайтов в разных странах и аспектами информационной культуры. //Социальный мир человека. Вып. 5. Материалы 5-й Всероссийской научно-практической конференции с международным участием «Человек и мир: психология конфликта, неопределенности и риска инноваций». 17-19 апреля 2014 г., ИППСТ УдГУ, Ижевск: Издател. Дом ERGO, 2014. С. 255-260.

2. Фефилов А.В. Компьютеры, роботы и интернет: средства роста эффективности деятельности и отдыха или новые виды стрессоров? // Материалы Всероссийской научно-практической конференции молодых ученых «Психофизические и социально-психологические аспекты взаимодействия в системе «человек-машина» (9-10 июня 2014 г.) / Отв. ред. А.В. Моров. – НОУ ВПО «Восточно-Европейский Институт», Институт Практической психологии МВЕУ. Ижевск: Издател. “Монпоражен», 2014. - 120 с. С. 69-73.

3. Фефилов А.В. Психофизиоинформационное взаимодействие: различные аспекты и проблемы понимания человека и языка компьютером.// Восточно-Европейский Научный Вестник. Глав. ред.

А.В. Моров. – НОУ ВПО «Восточно-Европейский Институт», Ижевск: Издат. ВЕИ, 2015. С. 64-68.

4. Яремчук С.А. Защита вашего компьютера от сбоев, спама, вирусов и хакеров на 100 %. – СПб.: Питер, 2007. – 288 С.

5. «Большой брат следит за тобой». Журнал CHIP № 11, 2013: С. 42-46.

6. «Хакеры и их приемы». Журнал CHIP № 11, 2013: С. 40-42 .

7. «Устраняем уязвимости в Android и iOS». Журнал CHIP № 8, 2015: С. 68-73.

8. «Добро пожаловать в машину». Журнал CHIP № 06, 2016, С.22-26.

9. «Техника лишает нас рассудка?» Журнал CHIP № 09, 2016, С.16-18.

10. «Цифровая агрессия». Журнал CHIP № 11, 2016, С. 22, 22-24.

11. «Меня взломали?» Журнал CHIP № 6, 2017: С. 52-59.

12. Яндекс новости. URL: https://news.yandex.ru/yandsearch?lr=44&cl4url=www.m24.ru%2Farticles%2F141000&lang=ru&rubric=computers&from=index

13. Яндекс новости. URL: https://news.yandex.ru/yandsearch?lr=44&cl4url=www.gazeta.ru%2Ftech%2Fnews%2F2017%2F05%2F25%2Fn_10092317.shtml&lang=ru&rubric=computers&from=index

14. Мейл.ру новости. URL: https://news.mail.ru/economics/30206649/?frommail=1

15. РБК Новости. URL: http://www.rbc.ru/technology_and_media/28/06/2017/5953a8c69a79472844f7c6d0?from=main

16. Новости cnews. URL: http://safe.cnews.ru/news/top/2017-06-09_eksperty_vyyasnilikakaya_os_stanet_novoj_zhertvoj

17. Новости cnews. URL: http://www.cnews.ru/news/top/2017-07-20_najden_sposob_obojti_vse_antivirusy_dlya_android