Информационная безопасность: психологические аспекты

А. Е. Войскунский

Войскунский Александр Евгеньевич
кандидат психологических наук, старший научный сотрудник кафедры общей психологии факультета психологии МГУ им. М.В. Ломоносова.

Проблема безопасности не принадлежит к числу фундаментально разработанных в психологической науке направлений. Тем не менее, в наши дни эта тематика становится одним из наиболее актуальных направлений психологических исследований. Мы придерживаемся следующей теоретической позиции, высказанной нами ранее [8] и базирующейся на психологии мотивации: безопасность – фундаментальная человеческая потребность. Согласно иерархии А. Маслоу [26], высшие человеческие потребности в самоактуализации, в признании и оценке, в любви и привязанности реализуются на основе удовлетворения физиологических (так называемых «витальных») потребностей человека, а также присущей каждому из нас потребности в безопасности.

Клинические данные свидетельствуют, что несоблюдение условий личной и/или групповой безопасности самым негативным образом сказывается на психическом развитии и психологическом здоровье индивидуума и социума. Причем потенциальными источниками угроз для личности или общества могут выступать любые непосредственные и опосредствованные взаимодействия: с другими людьми, группами людей, с многочисленными техническими устройствами (от настольных и переносных компьютеров до предприятий атомной энергетики), с разнообразными явлениями живой и неживой природы, с непрерывно усложняющимися знаковыми системами и т. п.

Специалистам удалось с разной степенью детальности описать ряд распространенных фобий, опасений и страхов, которые встречаются у их пациентов. Например, страх высоты – акрофобия, страх глубины – батофобия, боязнь замкнутых пространств – клаустрофобия, страх пустых пространств – кенофобия, боязнь общественных мест – агорафобия. Ряд опасений связан с нежеланием взаимодействия с животными – зоофобия. Весьма распространенные фобии касаются таких представителей фауны, как жуки – акарофобия, змеи – офидиофобия, пауки – арахнеофобия, клещи – акарофобия, собаки – кинофобия. Отмечается боязнь сезонных явлений природы: грома и грозы – астрафобия или бронтофобия, дождя и ливня – омрофобия, ветра – анемофобия. Встречаются страхи, вызванные разнообразными видами технических сооружений и машин. Среди них: боязнь средств транспорта (самолетов, метро и поездов, лифтов и т. п.) – амаксофобия; опасения, связанные с компьютерами, – киберфобия, компьютерная тревожность, техностресс и др.

Проблема безопасности получила определенное развитие как в зарубежной, так и в отечественной науке [27, 33]. Наряду с общеметодологическими аспектами данной проблемы изучаются и собственно психологические [15, 16, 23, 29, 32], в том числе связанные с психологической стороной такого явления, как терроризм [19, 21]. Эта тематика достаточно хорошо отражена в научной ли-

тературе. Поэтому мы обратимся к менее изученному отечественной психологической наукой направлению – психологии безопасности в сфере новых информационных технологий (часто именуемой «кибербезопасностью»).

Вопреки распространенному мнению [30] о том, что информационные воздействия (в частности, в рамках так называемых «информационных войн») имеют преимущественно «кибернетическую» природу, мы считаем, что исследования информационной безопасности должны опираться и на психологические данные. Проблема безопасности междисциплинарна по своей сути, поэтому и ее разработка должна носить комплексный и междисциплинарный характер.

Процессы глобализации напрямую связаны с появлением интернета и связанных с ним многочисленных мультимедийных сервисов. При этом сами технологии, как это отмечалось нами ранее [4, 17], амбивалентны относительно направлений психологического развития человека и человечества и, в первую очередь, молодого поколения, в значительной своей части в совершенстве овладевшего «компьютерной грамотностью». Вызванное и обусловленное применением информационных технологий (ИТ) психологическое развитие может пойти по позитивному, нейтральному или негативному пути, хотя сами по себе компьютеры, операционные системы, браузеры, языки программирования и интернет не определяют направления развития субъекта и общества в целом.

Существует ряд перспективных направлений развития одаренных в сфере ИТ детей и подростков [3, 36]. В то же время, имеются направления психологического развития, обусловленные информационными технологиями, которые можно смело отнести к числу негативных. Среди них: потенциальная (хотя и не всеми специалистами признаваемая) «интернет-аддикция» – зависимость от компьютера и интернета [22]; нередко доходящая до тяжелых стрессов компьютерная тревожность [7, 18]; своеобразная технократизация мышления [20], причем не обязательно свойственная специалистам, систематически работающим с техническими орудиями, и т. п. Отдельное и весьма неоднозначное место в этом ряду занимает хакерство [11, 13, 57, 51]. В данной статье мы уделим ему особое внимание.

Рассмотрим примерный перечень неправомерных, неэтичных и/или прямо криминальных применений современных ИТ. Такого рода данные анализируются специалистами в области компьютерной безопасности, юриспруденции, человеко-машинного взаимодействия, социологии, а с недавних пор – и в области философской этики.

Психология и обучение кибер-этике

Одно из современных направлений изучения особенностей морального поведения в интернете все чаще именуется кибер-этикой. Под ней понимаются правила морального (т. е. правильного, честного, справедливого) поведения в среде интернета. К сожалению, специалисты по этике и философы не пришли к универсально признанному мнению относительно определения «морали». Для наших целей *мораль* может быть определена «как система правил, управляющих человеческим поведением, а также принципов оценки этих правил» [52]. Многие авторы [42] вводят связанные с кибер-этикой вопросы в разряд актуальных морально-нравственных проблем, порожденных развитием технологий. Они обсуждают специфические направления научной и практической работы, сложившиеся в сфере изучения морального/аморального применения компьютеров и интернета, связанные, прежде всего, с предупреждением преступлений и обмана, возможностями защиты от них и обеспечения безопасности.

Активно обсуждаются [10, 9], например, меры противодействия порнографии, педофилии, сексуальным домогательствам посредством интернета, способы защиты детей от возможного ущерба их психическому здоровью, наносимого злоумышленниками. Большое внимание уделяется мерам противодействия обману и жульничеству в интернете, «захвату» (недобросовестной регистрации) потенциально привлекательных доменных имен с целью их последующей перепродажи, получению несанкционированного доступа к удаленным компьютерам, изощренному (или основанному на человеческой невнимательности либо доверчивости) воровству номеров кредитных карт (и, соответственно, денег, услуг, товаров), а также всем разновидностям плагиата, пиратства и нарушений авторского права.

Обсуждаются также вопросы о недопустимости ограничения личной свободы пользователей интернета в целях борьбы с «кибер-терроризмом» и о неправомерном использовании служебных компьютеров. Отмечается ущерб, наносимый либеральным ценностям, мерами контроля со стороны администрации за поведением сотрудников в интернете. Исследователи не обходят вниманием проявления хакерства, «правого» и «левого» экстремизма в интернете, намеренной диффамации (нанесения урона репутации), шантажа, «кибер-преследования» другого человека и связанных с этим угроз или ущемления свободы его/ее личности (privacy). Изучаются получившие в последнее время широкое распространение такие неэтичные и противозаконные действия, как: рассылка спама, составление и распространение компьютерных вирусов, установление контроля над удаленными компьютерами, разрушительные действия посредством компьютерных программ типа vandalware, создание проблем в функционировании удаленных веб-серверов (организация их перегруженности посредством направления многочисленных запросов – вызывание т. н. denial of service) и т. д.

Специалисты по обеспечению безопасности не прекращают попыток отслеживания секретной (например, посредством стеганографии) переписки между членами террористических групп, перекрытия каналов распространения информации об изготовлении поражающих веществ («рецептов» взрывчатых веществ типа «коктейля Молотова»), предупреждения распространившихся в последнее время призывов к совершению коллективных самоубийств, а также мониторинга [58] расистских, ксенофобских, воинственных и подобных выступлений.

Ученые стараются создавать теоретические модели в области кибер-этики. Например, Р. Мэйсон с соавторами выделяет следующие аспекты кибер-этичного поведения: доступность, точность, личная свобода и собственность [45]. Помимо универсальных нравственных принципов разработаны и постоянно дополняются кодексы профессиональной этики, в частности, в сфере информатики и компьютерных наук и в сфере управления информационными системами [1, 37, 41, 48]. Изучаются и неформальные групповые «кодексы», согласно которым хакеры «старой школы», отрицая даже самые распространенные этические нормы, тем не менее, руководствуются чем-то вроде «профессионального кода поведения» [11, 31].

Кроме того, в области кибер-этики проведены определенные эмпирические исследования [1, 9]. Например, установлено, что незаконные действия, связанные с использованием компьютеров (от незаконного копирования лицензионных программ до изменения или воровства компьютерных данных, содержащихся в чужих компьютерах), широко распространены среди школьников [47]. Показано, что студенты университетов с готовностью идут на ложь, связанную с применением информационных тех-

нологий (например, копируют электронные таблицы, компьютерные программы, предоставляют другим студентам незаконный доступ к электронным учебникам, скачивают и пытаются продать музыкальные CD). При этом полученная ими выгода ничтожна или невелика [49]. На процесс нравственного выбора в сфере ИТ селективно (т. е. в различных комбинациях) влияют: юридические, профессиональные факторы и социальное окружение, а также факторы, относящиеся к сфере личных убеждений: религиозные и нравственные ценности, особенности жизненного опыта [37].

Принято считать, что весьма существенными являются также культурные особенности применения ИТ. Эмпирически доказано [40], что индивидуальные религиозные представления (например, такие, как распространенная в Индии вера в реинкарнацию) влияют на вероятность пиратских действий и нарушений прав собственности в сфере информационных технологий.

Проведенное в Корее исследование показало высокую значимость пола, возраста и положения в социальной иерархии для осуществления морального выбора взрослыми респондентами [43]. В исследовании, в котором приняли участие студенты и сотрудники одного из университетов Таиланда, было продемонстрировано [44] значение демографических параметров (возраст, пол, социальный статус, т. е. место работы или год обучения) и опыта применения компьютеров для оценки моральной приемлемости фактов пиратства компьютерных программ. Отношение к нарушению прав собственности в области ИТ определяется следующими тремя факторами: субъективно воспринимаемым личным выигрышем (например, социальное принятие подобных действий, возврат долга, вежливая услуга); альтруизмом; субъективно воспринимаемыми негативными последствиями (если при этом опустить вопрос о законности или незаконности таких действий) [35].

Значимый вывод заключается в том, что никакая нация и никакая группа населения не является носителем перверсивного, т. е. полностью превратного толкования морально-нравственных принципов в данной области. Об этом свидетельствуют результаты обширного (проведенного в 9 странах) кросскультурного исследования [59].

Одно из центральных положений данной работы состоит в том, что новейшие проблемы, связанные с кибер-этикой, существенным образом пересекаются с проблемами психологии – как общей, так и психологии развития. Согласно проведенным нами пилотажным исследованиям [53, 55], компетентные в использовании интернета подростки (учащиеся старших классов средней школы) при ответе на прямые и/или косвенные вопросы допускают возможность выполнения ими неэтичных или противозаконных действий в виртуальной среде, в частности, направленных на другого человека. При этом они никогда не допускают выполнения аналогичных действий в реальной жизни. Напрашивается предположение: школьники, студенты, а нередко и люди зрелого возраста неспособны перенести вполне известные им (применительно к хорошо знакомым ситуациям) этические нормы в новую, недостаточно пока что знакомую (виртуальную) среду.

На наш взгляд, подобное предположение объясняет значительную долю случаев неэтичного поведения в интернете. Такое поведение свидетельствует о неспособности предвидеть последствия своих действий, нести компетентную ответственность за неэтичные поступки. Непреднамеренные правонарушения могут оказаться также результатом небрежности, моральной незрелости, безразличия, недостатка любопытства, а часто – просто невежества. Неосведомленность может быть связана с психологической неспособностью проявить должную гибкость и перенести хорошо освоенные поведенческие механизмы в новую ситуацию. Этические нормы, в соответствии с которыми действует конкретный субъект, как известно, не всегда являются в достаточной степени гибкими. Они складываются в течение длительного времени, проходя при этом определенные стадии развития.

Если обратиться к соответствующим психологическим теориям и фактам, то наиболее основательно разработанной оказывается когнитивно-развивающей теория морального развития Л. Колберга [45], в значительной мере опирающаяся на основополагающие труды Ж. Пиаже [28]. Согласно ей, имеются три стадии морального развития: дотрадиционная мораль, традиционная мораль и посттрадиционная мораль (в каждой стадии есть по две подстадии). При этом сравнительно немногие взрослые люди достигают в своем нравственном развитии высшей стадии, а их реальное поведение не всегда оказывается на высоте достигнутой стадии морального развития. К тому же «...результативность решения моральных проблем предполагает умение вести диалог и сближать противоположные точки зрения» [2], а группа или партнер могут способствовать высокоморальному или недостаточно моральному поведению как на высокой, так и на низкой стадии морального развития.

Наряду со стадиальностью развития моральные нормы характеризуются степенью гибкости, которая определяется моральными рассуждениями и/или поведением, соответствующим достигнутой стадии морального развития в новых и малознакомых ситуациях. Так, известны случаи одичания в сообществах, подвергшихся длительной изоляции. Не менее известны примеры высокоморального поведения в трудных, нечеловеческих условиях [34]. Моральная гибкость, или способность к переносу известных моральных норм в незнакомые ситуации, характерна для разных людей в различной степени.

Мы предполагаем, что недостаточная гибкость моральных норм в области ИТ может быть компенсирована специальным обучением (тренингом). Такое обучение может и должно способствовать переносу уже известных субъекту моральных норм в среду применения информационных технологий. Это достаточно друдная, но неотложная задача. В первую очередь в ней нуждаются представители молодого поколения – дети и подростки. Острая необходимость такого обучения была обоснована отечественными авторами [3, 5, 6, 10]. При подготовке к организации подобного тренинга нетрудно воспользоваться тем, что подростки уже являются субъектом регулярной системы обучения. Обучающий курс (возможно, факультативный) должен быть основан на разборе конкретных ситуаций с последующим подведением учащихся к самостоятельным выводам. Этот курс должен быть дифференцированным в зависимости от психологического возраста обучаемых и от уровня их морального развития, измеряемого, например, в соответствии со стадиальной системой Л. Колберга. Насколько известно, за рубежом целостная обучающая система такого рода отсутствует, зато есть немало пособий для родителей и преподавателей, которые хуже детей разбираются в информационных технологиях [50].

Такая образовательная программа должна быть ориентирована на интернациональную аудиторию. В обучении кибер-этике подрастающих поколений больше заинтересованы развитые страны, поскольку именно находящиеся там объекты чаще всего выступают в качестве наиболее привлекательных целей кибер-атак, осуществляемых хакерами-разрушителями. Последних было бы правильнее именовать в силу специфики выполняемых ими действий не родовым и обобщенным наименованием «хакеры», а наименованием «кракеры», от-

носящимся исключительно к хакерам-разрушителям (в то время как остальные хакеры даже приносят определенную помощь обществу [14]).

В то же время, имеет место не вполне правомерная, на наш взгляд, попытка обозначения «социальными хакерами» [24] разнообразных обманщиков, манипуляторов, специалистов по некорректному, корыстному применению методов социальной инженерии. Эти методы могут быть как связанны с применением разнообразных информационных технологий, выполняемых в сфере «киберпространства», так и совершенно не имеющими отношения ни к ИТ, ни к условным рамкам «киберпространства».

Непреднамеренные правонарушения могут оказаться также результатом небрежности, моральной незрелости, безразличия, недостатка любопытства, а часто – просто невежества. Неосведомленность может быть связана с психологической неспособностью проявить должную гибкость и перенести хорошо освоенные поведенческие механизмы в новую ситуацию.

«Опыт потока» в деятельности хакеров

Обратимся к отмеченным выше исследованиям мотивации хакерского поведения, а именно к изучению мотивации потока в деятельности хакеров [13, 57, 56]. Основополагающие представления об опыте потока были введены три десятилетия назад в трудах М. Чиксентмихайи [39, 38] – одного из основоположников позитивной психологии.

Опыт потока понимается М. Чиксентмихайи, его коллегами и учениками как специфическое состояние полной поглощенности деятельностью, в котором действие следует за действием согласно своей внутренней логике, а результат деятельности и ее реальная продолжительность отходят в сознании субъекта на второй план. При этом деятельность захватывает субъекта, выполняется с радостью и удовольствием без заботы о ее конечном результате. Опыт потока и радость от его переживания способствуют возникновению мотивации, побуждающей и в дальнейшем переживать этот опыт, стремиться выполнять соответствующую деятельность.

В данной работе мы не будем останавливаться на подробном анализе психологических детерминант опыта потока. Отметим только вслед за М. Чиксентмихайи, что характерным для этого состояния принято считать возникновение и сохранение баланса между наличествующими у субъекта навыками и выдвигаемыми им целями. Баланс свидетельствует о том, что выдвигаются цели, для реализации которых имеются соответствующие навыки, и что эти навыки и умения используются для реализации таких целей, которые не могут быть названы ни чересчур сложными (иначе цели не могли бы быть реализованы), ни упрощенными (иначе избыточные навыки не позволили бы достигнуть желаемого баланса и, стало быть, состояния потока) [12, 25]. Итак, опыт потока означает хрупкое равновесие между требованиями ситуации и собственными возможностями (умениями, знаниями, навыками и т. п.), при этом и те и другие должны находиться на пределе порогового для данного человека уровня.

Существенным элементом опыта потока следует признать быструю обратную связь, характеризующую успешность или неуспешность предпринимаемых действий. Поскольку в условиях применения ИТ канал обратной связи может быть организован без большого труда, то исследователями неоднократно предпринималось изучение свойств опыта потока в деятельности, опосредствованной компьютерами и интернетом [54].

Остановимся на интерпретации результатов проведенного исследования деятельности хакеров в контексте психологии безопасности [13, 57, 56, 51]. В этом исследовании приняли участие 457 респондентов, половина из которых охарактеризовала себя как высококвалифицированных специалистов, в то время как другая половина уступала им по квалификации. Гипотеза эмпирического исследования состояла в том, что для деятельности хакеров характерен опыт потока, причем для высококвалифицированных респондентов опыт потока должен быть характерен в более высокой степени, чем для менее квалифицированных. Работа была выполнена с помощью метода ретроспективного опроса [12].

Опыт потока, как показали полученные результаты, присущ деятельности хакеров, при этом не имела место линейная зависимость между квалификацией (навыками и умениями) и опытом потока. Зависимость между сложностью выдвигаемых целей и соответствующими таким целям навыками более сложна, чем предполагалось. Такую зависимость справедливо было бы именовать динамической, поскольку она отражает динамику развития переживания опыта потока в поведении хакеров соответственно их квалификации и реализуемым целям.

Предположительная динамика развития переживания опыта потока в деятельности хакеров представляется следующей. На начальном этапе активности в качестве хакера степень знакомства с продуктами информационных технологий обычно бывает невысока. Поскольку освоение наиболее простых специализированных хакерских программ не требует, согласно всеобщему мнению, глубоких знаний в сфере ИТ и высокой программистской квалификации, то новичок, ставя перед собой посильные задачи, нередко справляется с ними, увлекается данной активностью и неожиданно для себя испытывает переживание, близкое по феноменологии к мотивации потока: и цели деятельности, и наличные навыки невысоки и всецело соответствуют друг другу.

Если подобное переживание фиксируется, то хакер надолго остается на начальной стадии специфических хакерских и/или программистских умений и навыков. Судя по литературным данным, не утруждающие себя существенным повышением программистской квалификации хакеры весьма многочисленны.

Динамика проявляется в том, что реализуемые новичком цели могут постепенно усложняться, не нарушая баланс между имеющимися навыками и уровнем сложности выбираемых задач. Таково наиболее, пожалуй, комфортное направление динамики опыта потока для хакера-новичка: совершенствование имеющихся у него знаний и умений сопровождается посильным усложнением выдвигаемых целей, при этом сохраняется и фиксируется желанное и высоко ценимое переживание опыта потока.

Судя по ретроспективным данным (был осуществлен выборочный постэкспериментальный опрос респондентов), подобное эволюционное сохранение опыта потока представляет собой до-

вольно редкое исключение. Действительно, постоянное (поэтапное) соблюдение тонкого баланса между растущими умениями и изменчивыми целями деятельности представляется делом непростым. Много чаще, как отмечают респонденты, имеет место временный или постоянный перерыв в переживании опыта потока из-за несоответствия целей деятельности возросшим навыкам либо из-за несоответствия низких навыков завышенным и нереалистичным целям деятельности.

Итак, могут быть отмечены следующие варианты утраты опыта потока. Во-первых, это повышение квалификации в применении ИТ, не сопровождающееся изменением целей и хакерских задач. В этом случае разрушается баланс между уровнем сложности задач и наличными навыками: простые хакерские задачи перестают сопровождаться опытом потока, и хакерство утрачивает свою привлекательность. Таков путь к постепенному уходу из хакерского сообщества: он неоднократно описан бывшими хакерами, переквалифицировавшимися, например, в специалистов в области защиты информации (в частности, от хакерских вторжений). В отдельных случаях, как показывает опыт, возникает «рецидив» хакерского подхода, когда ставятся соответствующие высоким навыкам цели и вновь переживается опыт потока. Насколько можно судить, подобные нечастые возвраты к хакерским действиям бывают обусловлены некоторыми внешними причинами (например, желанием отомстить обидчику – работодателю, агрессору).

Во-вторых, немотивированное усложнение хакерских целей и задач без сопутствующего повышения программистской квалификации. В этом случае хакер действует «на авось», успехи его обычно невелики, опыт потока исчезает или становится редкостью. Скорее всего, малоквалифицированному хакеру с завышенными притязаниями не удастся самореализоваться в хакерском сообществе, хотя в случае повышения квалификации баланс между умениями и целями может быть достигнут на новом уровне.

И, в-третьих, это вскрытый в нашем исследовании механизм периодической утраты мотивации потока в результате дисбаланса решаемых задач и наличных навыков, после чего баланс – уже на новом уровне знаний и притязаний – достигается вновь и сопровождается повторным обретением опыта потока. Процесс этот может повторяться много раз. На основании результатов проведенного исследования можно предполагать, что таков ведущий механизм квалифицированного хакерства.

Выводы

Наиболее желательным направлением динамики хакерской деятельности является движение от начинающего хакера к эпизодическому хакеру и, вероятнее всего, к постепенному уходу из хакерского сообщества и присоединению к сообществу квалифицированных специалистов в области ИТ. Нам представляется, что одним из средств выполнения задач программы обучения основам кибер-этики может стать демонстрация подросткам, которые уже испытали свои силы в хакерской деятельности, преимуществ приведенной выше динамики. Такая динамика вполне реалистична, она может быть проиллюстрирована рядом биографических примеров – например, жизненных перипетий Кевина Митника и других получивших громкую известность хакеров. Подобный курс обучения в рамках программы знакомства с основами кибер-этики может быть предназначен для тех учащихся, которые уже попробовали свои силы в хакерской деятельности или планируют сделать это.

Такой подход сможет повлиять на хакеров-новичков и на будущих хакеров, помочь им осуществить перенос знакомых по обыденной жизни норм морали в ситуации, связанные с пребыванием в виртуальной среде. Предполагаемая направленность такой обучающей программы на профилактику хакерства неслучайна: во-первых, хакерство считается среди молодежи модным стилем поведения, а во-вторых, хакерство (читай: кракерство) считается весьма тяжелым случаем правонарушения. Однако не следует забывать, что помимо хакерства имеется целый ряд других противоправных форм применения информационных технологий. Поэтому предполагается, что обучающий курс будет направлен на профилактику большинства или всех (по возможности) разновидностей таких действий.

Задачей такого обучения является резкое снижение числа новичков (из представителей подрастающего поколения), которые практикуют противоправные применения компьютеров, интернета и т. п. На наш взгляд, речь может и должна идти не столько о борьбе с начинающими (еще не «профессионализировавшимися») хакерами, сколько об их воспитании и перевоспитании. Даже если подобные меры перевоспитания окажутся малоэффективными для изменения жизненных установок убежденных «закоренелых» хакеров, все же они представляются чрезвычайно полезными, поскольку способны привести к сокращению числа начинающих хакеров. А при отсутствии обеспеченного притока новичков любое сообщество теряет перспективу. Составление и реализация подобной программы повсеместного обучения представляется более гуманным по отношению к подрастающему поколению методом борьбы с нарушениями в компьютерной сфере, нежели практикуемый в настоящее время полицейско-юридический подход. К тому же, психолого-педагогическое воздействие в виде разработанных для детей и подростков специальных обучающих программ по основам кибер-этики можно смело признать более дешевым способом защиты информации, чем постоянно растущие затраты на технические средства защиты.

Литература

1. Алексеева И.Ю., Шклярик Е.Н. Что такое компьютерная этика? // Вопросы философии. – 2007. – №9. – С. 60–72.
2. Анцыферова Л.И. Связь морального сознания с нравственным поведением человека (по материалам исследований Лоуренса Колберга и его школы) // Психологический журнал. – 1999. – Т. 20. – №3. – С. 10.
3. Бабаева Ю.Д., Войскунский А.Е. Одаренный ребенок за компьютером. – М: Сканрус, 2003.
4. Бабаева Ю.Д., Войскунский А.Е. Психологические последствия информатизации // Психологический журнал. – 1998. – Т. 9. – №1. – С. 89–100.
5. Бондаренко С.В. Киберэтика и сетевые сообщества (молодежный аспект проблемы с точки зрения американских социологов и психологов) // Социальные и психологические последствия применения информационных технологий: Матлы международной Интернет-конференции / Под ред. А.Е. Войскунского. – М., 2001. – С. 243–252.
6. Бондаренко С.В. Социальная струкутра виртуальных сетевых сообществ. – Ростов-на-Дону: Изд-во Ростовского университета, 2004.
7. Васильева И.А., Пащенко Е.И., Петрова Н.Н., Осипова Е.М. Психологические факторы компьютерной тревожности // Вопросы психологии. – 2004. – №5.
8. Войскунский А.Е. Психологические аспекты информационной безопасности // Глобальная информатизация и безопасность России. – М.: Изд-во Московского университета, 2001. – С. 168–175.
9. Войскунский А.Е., Дорохова О.А. Становление киберэтики: исторические основания и современные проблемы // Вопросы философии. – 2010. – №5.
10. Войскунский А.Е., Нафтульев А.И. Актуальные психологические проблемы кибер-этики // Гуманитарная информатика. Вып. 3 – Томск: Изд-во Томск. ун-та, 2007. – С. 31–39.
11. Войскунский А.Е., Петренко В.Ф., Смыслова О.В. Мотивация хакеров: психосемантическое исследование // Психологический журнал. – 2003. – Т. 24. – №1. – С. 104–118.

12. Войскунский А.Е., Смыслова О.В. Мотивация потока и ее изучение в деятельности хакеров // Современная психология мотивации / Под ред. Д.А. Леонтьева. – М.: Смысл, 2002. – С. 244–277.
13. Войскунский А.Е., Смыслова О.В. Роль мотивации «потока» в развитии компетентности хакера // Вопросы психологии. – 2003. – №4. – С. 35–43.
14. Геринг В.Г. Оказывают ли хакеры услугу обществу? // Интернет в общественной жизни. – М.: Идея-Пресс, 2006. – С. 55–71.
15. Глобальная информатизация и безопасность России. – М.: Изд-во Московского университета, 2001.
16. Грачев Г.В. Личность и общество: информационно-психологическая безопасность и психологическая защита. – М.: Per Se, 2003.
17. Гуманитарные исследования в Интернете / Под ред. А.Е. Войскунского. – М.: Терра-Можайск, 2000.
18. Доронина О.В. Страх перед компьютером: природа, профилактика, преодоление // Вопросы психологии. – 1993. – №1. – С. 68–78.
19. Ениколопов С.Н., Мкртычян А.А. Психологические последствия терроризма // Вопросы психологии. – 2008. – №3. – С. 71–80.
20. Зинченко В.П., Моргунов Е.Б. Человек развивающийся. Очерки российской психологии. – М., 1994.
21. Зинченко Ю.П., Шилко Р.С. Выявление групп риска, представляющих ресурсы развития терроризма, и обоснование принципов антитеррористической деятельности на этом направлении // Современный терроризм и борьба с ним: социально-гуманитарные измерения / Под ред. В.В. Ященко. – М., 2007. – С. 35–52.
22. Интернет-зависимость: психологическая природа и динамика развития / Под ред. А.Е. Войскунского. – М., 2009.
23. Информационная и психологическая безопасность в СМИ: В 2-х томах. – Т. 1: Телевизионные и рекламные коммуникации / Под ред. А.И. Донцова, Я.Н. Засурского, Л.В. Матвеевой, А.И. Подольского. – М.: Аспект Пресс, 2002.
24. Кузнецов М., Симдянов И. Социальная инженерия и социальные хакеры. – СПб: БХВ-Петербург, 2007.
25. Макалатия А.Г. Опыт аутотелической деятельности // Общая психология. Тексты: В 3 т. – Т. 2: Субъект деятельности. – Книга 2. – Изд. 2-е, испр. и доп. / Отв. ред. В.В. Петухов. – М.: УМК «Психология», 2004. – С. 264–278.
26. Маслоу А.Г. Мотивация и личность. – СПб: Евразия, 2001.
27. Научные и методологические проблемы информационной безопасности / Под ред В.П. Шерстюка. – М.: Изд-во МЦНМО, 2004.
28. Пиаже Ж. Моральное суждение у ребенка. – М.: Академический проект, 2006.
29. Проблемы информационно-психологической безопасности / Под ред. А.В. Брушлинского и В.Е. Лепского. – М.: ИП РАН, 1996.
30. Расторгуев С.П. Информационная война. – М.: Радио и связь, 1998.
31. Рэймонд Э.С. Новый словарь хакера. – М.: ЦентрКом. 1996.
32. Смолян Г.Л., Зараковский Г.М., Розин В.М., Войскунский А.Е. Информационно-психологическая безопасность (определение и анализ предметной области). – М.: Ин-т системного анализа РАН, 1997.
33. Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы / Под ред. В.А. Садовничего и В.П. Шерстюка. – М.: Изд-во МЦНМО, 2002.
34. Франкл В. Сказать жизни «Да»: психолог в концлагере. – М.: Смысл, 2004.
35. Ang A.Y., Lo B.W.N. Software piracy attitudes of tertiary students in Australia. – 2001. – http://www.hkcs.org.hk/searcccd/ed11_aa.htm
36. Babaeva J.D., Voiskounsky A.E. IT-Giftedness in Children and Adolescents // Educational Technology & Society. – 2002. – Vol. 5(1) – P. 154–162.
37. Cronan T. P., Kreie J. Making ethical decisions // Communications of the ACM. – 2000. – 43(12) – P. 66–71.
38. Csikszentmihalyi M. Beyond boredom and anxiety: experiencing flow in work and play. – San-Francisco: Jossey-Bass, 2000 (впервые издана в 1975 г.).
39. Csikszentmihalyi M. Flow: The Psychologi of Optimal Experience. – New York: Harper and Row, 1990.
40. Debnath N., Bhal K.T. Religious belief and pragmatic ethical framework as predictors of ethical behavior // Cultural Attitudes towards Technology and Communication / F. Sudweeks, Ch. Ess (Eds.). Proceedings of the 3rd International Conference – Montreal, Canada, 12–15 July, 2002. – P. 409–420.
41. Grodzinsky F.S. The development of the "ethical" ICT professional and the vision of an ethical on-line society: how far have we come and where are we going? // ACM SIGCAS Computers and Society. – 2000. – 30(1). – P. 3–7.
42. Hamelink C.J. The Ethics of Cyberspace. London, Thousand Oaks, New Delhi: Sage, 2000; Internet Ethics / Langford D. (Ed.). – Houndmills et al.: Macmillan Press, 2000.
43. Kim K.H. A study of the conduct of Korean IT participants in ethical decision making // Lecture Notes in Computer Science, 2713. – 2003. – P. 64–74.
44. Kini R.B., Ramakrishna H.V., Vijayarama B.S. An Exploratory Study of Moral Intensity Regarding Software Piracy of Students in Thailand // Behaviour & Information Technology. – 2003. – Vol. 22. – №1. – P. 63–70.
45. Kohlberg L. The Meaning and Measurement of Moral Development. – Clark Univ. Press, 1981.
46. Mason R.O., Mason F.M., Culnan M.J. Ethics of Information Management. – Thousand Oaks, CA: Sage Publ., 1995.
47. McGuire Sh., D'Amico E., Tomlinson K., Brown S. Teenagers self-reported motivations for participating in computer crime // 8th International Conference on Motivation (Workshop on Achievement and Task Motivation). Abstracts. – Moscow, 2002. – P. 72–73.
48. Panteli A. Code Confidential: Codes of Practice for Computing Professionals. // ACM SIGCAS Computers & Society. – 2003. – 32(6). – http://ww.computersandsociety.org/AccessController/sigcas/subpage/sub_page.cfm?article=844&page_number_nb=1
49. Ruf B.M., Thomas S.B. Unethical decision-making with computer usage in a university environment. 2003. – http://aaahq.org/AM2003/EthicsSymposium/Session%205a3.pdf
50. Schwartau W. Internet & Computer Ethics for Kids. – Interpact, 2001.
51. Smyslova O.V., Voiskounsky A.E., Petrenko V.F. Hackers' Motivation: Empirical Study // Psychology in Russia: State of the Art / Ed. by Y. Zinchenko & V. Petrenko. – Moscow: Department of Psychology MSU & IG-SOCIN, 2008. – P. 224–238.
52. Tavani H.T. Ethics & Technology: Ethical Issues in the Age of Information and Communication Technology. – N.Y. et al.: Wiley, 2004. – P. 28.
53. Voiskounsky A. Current problems of moral research and education in the IT environment // Human Perspectives in the Internet Society: Culture, Psychology and Gender / K. Morgan, C.A. Brebbia, J. Sanchez, A.Voiskounsky (eds.). WIT Press: Southampton. – Boston, 2004. – P. 33–41.
54. Voiskounsky A.E. Flow Experience in Cyberspace: Current Studies and Perspectives. // Psychological Aspects of Cyberspace: Theory, Research, Applications. / Ed. by A. Barak. – N.Y.: Cambridge University press, 2008. – P. 70–101.
55. Voiskounsky A.E. Virtual Environments: the need of advanced moral education // Ethics of New Information Technology. Proceedings of the 6th International Conference of Computer Ethics: Philosophical Enquiry (CEPE2005). / Ed. by Ph. Brey, F. Grodzinsky, L. Introna. Enshede, the Netherlands: CTIT Publ., 2005. – P. 389–395.
56. Voiskounsky A.E., Smyslova O.V. Flow in computer hacking: A model // Lecture Notes in Computer Science. – Vol. 2713. – 2003. – P. 176–186.
57. Voiskounsky A.E., Smyslova O.V. Flow-Based Model of Computer Hackers' Motivation // CyberPsychology & Behavior – 2003. – Vol. 6. – №3. – P. 171–180.
58. Weimann G. Terror online: How do terrorists use the Internet? // Countering Modern Terrorism: History, Current issues and Future Threats / K. von Knop, H. Neisser, M. von Creveld (eds.). Proceedings, 2nd International Security Conference (Berlin, 15–17 December 2004). – Bielefeld: W. Bertelsmann Verlag, 2005. – P. 87–109.
59. Whitman M.E., Townsend A.M., Hendrickson A.R. Cross-national differences in computer-use ethics: A nine-country study // Journal of International Business Studies. – 1999. – 30(4). – P. 673–687.