

*И. Ю. Алексеева*

## ОБ ЭТИЧЕСКОЙ СОСТАВЛЯЮЩЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ\*

Широкое видение информационной безопасности охватывает, наряду с проблемами надежной защиты информации, вопросы защиты людей и технических систем от разрушающего воздействия информации, а также задачи обеспечения требуемого качества информации [1. С. 5–8]. Противостояние дестабилизирующему воздействию на систему внешних и внутренних угроз, как и предотвращение порождаемых функционированием системы негативных последствий для внешней среды, так или иначе зависит от деятельности людей. Человек же в своих действиях руководствуется разнообразными мотивами, установками и интересами, соблюдает или нарушает определенные правила, в том числе юридические и этические.

Совершенствование средств правового регулирования в сфере информационных технологий — дело весьма важное, однако оно не может быть сосредоточено лишь на позитивном праве. Эффективность действия писаных законов оказывается под вопросом, если такие законы игнорируют сложившиеся представления людей о справедливости и разумности, о приемлемости тех или иных моделей поведения. Большое значение в данных условиях приобретают вопросы этические, ибо, во-первых, по-настоящему действенным может быть лишь закон, базирующийся на нравственных основаниях, а во-вторых, невозможно подвести под юридические нормы и проконтролировать все аспекты деятельности человека.

Развитие информационных технологий расширяет область анонимных действий. Фактор невидимости существенно влияет на представления о дозволенном и недозволенном, способствует

---

\* Работа выполнена при финансовой поддержке РГНФ. Проект № 09–03–00377а. Руководитель проекта — профессор А. А. Малюк.



формированию убеждения, что в киберпространстве перестают действовать обычные правила поведения.

Человек искренне недоумевает, когда из-за поступков, совершенных в виртуальном мире, становится объектом интереса правоохранительных органов, — ведь «в реале» он ничего противоправного не сделал!

Серьезное осмысление этических проблем не должно принимать форму морализаторства. Иногда в качестве универсального способа их решения предлагают аналогию с «реалом». Подобный подход оправдан, если речь идет о таких действиях, как взлом систем и баз данных, рассылка компьютерных вирусов, распространение руководств по изготовлению взрывных устройств. Однако возможности анонимности, предоставляемые современными информационно-коммуникационными технологиями, используются не только для достижения злонамеренных целей, но и в гораздо более широком круге ситуаций, когда прямой перенос регулятивов из «реала» невозможен или неуместен.

Нравственный смысл создания и применения техники традиционно определялся в контексте осуществления творческих возможностей человека, удовлетворения потребностей, ответственного отношения к вопросам, затрагивающим благополучие других людей, их здоровье, имущественные и иные интересы. Когда речь идет не о традиционной технической системе, границы которой проходят по стенкам корпуса машины [2. С. 34], а о качественно новом продукте инженерной и социотехнической деятельности, не имеющем четкой пространственно-временной локализации, то категории творчества, потребности и ответственности не переходят в разряд устаревших, однако их практические корреляты меняются. Развитие информационных технологий столь стремительно, что эффект быстрого устаревания распространяется и на соответствующие гуманитарные исследования. Показателен в данном отношении международный проект, результатом которого стало издание книги «Этика Интернета» британским издательством «Макмиллан» в 2000 г. [3] (автору данной статьи довелось поучаствовать в указанном издании в роли «комментирующего автора»). Учитывая быстрые изменения в Интернете, руководители проекта поставили задачу подготовить текст книги в течение полугода. Работа была спланирована таким образом из опасения, что при более длительных сроках подготовки книга окажется несвоевременной к моменту выхода в свет. Подобное положение дел оставляет ученому слишком мало времени на то, чтобы оглянуться на прошлое, проанализировать накопленный опыт, определить собственные методы и соотнести их с методами коллег. Это — трудности, относящиеся к академическим работам. Они никоим образом не отменяют актуальности и значимости усилий, направленных на осмысление изменений, происходящих в информационной культуре, попыток определить принципы и правила поведения в меняющихся условиях, дискуссий о нормах и ценностях.

Информационные технологии развиваются не в культурном вакууме и не являются единственным «культуропорождающим» фактором. В силу целого комплекса экономических, социальных, политических и конечно же технологических факторов усиливаются такие тенденции, как перемещение внимания субъекта с духовной, интеллектуальной сферы на материальную, телесно-вещную, трансформация культа знания и просвещения в культ удовольствия и естественности, освобождение от стремления к идеалу в пользу прагматизма и утилитаризма, подмена творчества потреблением, жизни — игрой, реальных отношений виртуальными [4. С. 22]. Эффективность в решении сиюминутных задач выдвигается в качестве основного критерия рациональности, подвергается сомнению статус истины как высшей познавательной ценности, мышление «освобождается от гнета» логических правил, вследствие чего стираются различия между независимостью мышления и интеллектуальным капризом. Подобные тенденции следует принимать во внимание, обсуждая этические аспекты информационной безопасности. При этом



стремление обеспечить чистоту «собственно этического» анализа, отвлекающегося от контекстов культурологических, психологических и теоретико-познавательных, вряд ли было бы оправданным и практически осуществимым.

Примером комплексной, междисциплинарной проблемы, имеющей важную этическую составляющую, является проблема информационно-психологической безопасности, т. е. сохранения психического и нравственного здоровья человека в условиях современной информационной среды, не только открывающей перед людьми новые возможности развития и самореализации, но и порождающей новые угрозы сознанию. Внимание к информационно-психологической безопасности как особому предмету исследования было привлечено в России в 90-е годы XX в. В 1995 г. Институтом психологии РАН была проведена 1-я научно-практическая конференция по проблемам информационно-психологической безопасности.

Тот факт, что тема информационно-психологической безопасности как особая тема зазвучала именно в нашей стране, не может считаться случайным. 90-е годы XX в. — время коренных изменений в политической, социальной и культурной сфере, сопровождавших превращение РСФСР из крупнейшей составной части Советского Союза в отдельное государство — Российскую Федерацию, столкнувшееся с новыми, непредвиденными и острыми проблемами. В их числе — проблемы предотвращения рискованных социально-психологических ситуаций, когда нарушения нравственных, правовых или технологических норм создают угрозы для нормальной жизнедеятельности социума. Наряду и в тесной связи с вопросами социально-психологической безопасности ставились вопросы защиты от манипуляций. В 90-е годы XX в. вчерашние советские люди, внимание которых прежде не было объектом конкурентной борьбы многих сил, организаций и лиц, преследующих различные политические и коммерческие цели, оказались практически беззащитными перед таким, новым для них явлением, как коммерческая реклама, и новыми формами политической пропаганды.

В условиях информационной эпохи объемы смысловой информации (слово «смысловая» трактуется в данном случае широко, охватывая не только текст, но также изображение и звук), передаваемой по техническим каналам связи, притом производимой и распространяемой специально созданными для этого организациями, растут гораздо быстрее, чем объемы смысловой информации, получаемой человеком из непосредственного опыта и личного общения. Поэтому в области социально-психологической безопасности и психологической защиты личности на первый план выдвинулись проблемы информационные.

Слово «психологическая» в составе термина «информационно-психологическая безопасность» не означает, что в комплексе соответствующих проблем нет таких, которые требуют внимания не только психологов, но и ученых других специальностей. Показательна в этом отношении позиция доктора психологических наук Г. В. Грачева. «Информационно-психологическая безопасность, — пишет он, — является предметом исследования ряда дисциплин гуманитарного профиля — философии, культурологии, психологии, социологии, политологии и др. Эти исследования носят междисциплинарный характер, но представляется возможным сгруппировать их и выделить как самостоятельное и важное направление науки и социальной практики. Данное направление, на наш взгляд, может плодотворно разрабатываться в рамках самостоятельной научной дисциплины, которую можно обозначить как социология информационно-психологической безопасности или социология информационно-психологической безопасности» [5. С. 14] (курсив Г. В. Грачева — И. А.). Ориентация на создание самостоятельной дисциплины в рамках социологии, безусловно, имеет свои основания. Но если такая дисциплина возникнет, это не будет означать, что проблемы информационно-психологической безопасности не смогут плодотворно изучаться исследователями, не принадлежащими к социологическому сообществу. В принципе, разработка проблематики информационно-психологической безопасности требует усилий представителей всех областей

знания, где изучаются феномены индивидуального и общественного сознания, природа ценностей (социальных, нравственных, эстетических), вопросы обеспечения успешной работы социально-политических систем и защиты таких систем от актуальных или потенциальных угроз.

Проблемы моральных прав и морального долга личности, достоинства человека и развития человека в данном контексте тесно связаны, а то и сливаются воедино с проблемами разумности, независимости мышления, сохранения психологического потенциала и выработки адекватной информационно-ориентированной основы поведения.

Следует согласиться с теми, кто считает интеллектуализацию личности важнейшим фактором обеспечения информационно-психологической безопасности, связывая интеллектуализацию с развитием способности анализировать информационную ситуацию, оценивать достоверность информации, выявлять манипулятивный характер информационно-психологических воздействий, вырабатывать наиболее приемлемые для данного человека способы защиты от нежелательных последствий [6. С. 67]. При этом справедливо подчеркивается роль жизненного опыта, воспитания и самовоспитания в формировании и развитии имманентно присущих человеку защитных свойств личности.

Вместе с тем было бы упрощением сводить угрозы информационно-психологической безопасности личности только к манипуляциям, т. е. к целенаправленным негативным информационно-психологическим воздействиям, сознательно осуществляемым неким субъектом в отношении группы, к которой данная личность принадлежит. Дело в том, что современная информационно-технологическая среда как таковая, открывая перед человеком широкие возможности для новых видов активности, содержит и потенциальные опасности деформаций в структуре личности и способах ее социальной адаптации. К таким деформациям относятся различные формы компьютерной зависимости, виртуализм, авитализм (утрата жизнеспасающих установок), клиповое мышление, примитивизация речи, ослабление памяти и отказ от развития способности к самостоятельному производству знаний в условиях расширяющегося доступа к информации.

Интеллектуализация личности, необходимая для преодоления подобного рода опасностей, неразрывно связана с развитием морально-волевых качеств человека. Для конкретизации задач и способов интеллектуализации представляется ценным предпринятое В. К. Финном [7. С. 89] уточнение совокупности способностей, образующих естественный интеллект. В числе таковых — способность выделять существенное в наличных данных и знаниях (необходимый аспект интуиции), способности к целеполаганию и планированию, к рассуждению, аргументированному принятию решений, к оценке знаний и действий, способность задавать вопросы «что такое?», «почему?» и искать ответы на них, способности к синтезу познавательных процедур, к обучению и использованию памяти, к рационализации идей, способность к созданию целостной картины предмета мышления и способность к адаптации в условиях изменения жизненных ситуаций и знаний.

Психология и этика защиты в информационно-технологическом контексте предполагают не просто выживание, но развитие (в том числе с использованием имеющихся и созданием новых информационных ресурсов и технологий), не изоляцию, но участие в процессах коммуникации, обновление информационных ресурсов за счет надежных данных, концептуальных структур и ценностных ориентиров, необходимых для эффективной организации опыта, адекватной постановки и решения задач.

## СПИСОК ЛИТЕРАТУРЫ:

1. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учебное пособие для вузов. М., 2004.



- 
2. Гаврилина Е. А. Виртуализация современных инженерных практик // Предпринимательство. Этика. Техника. 2007. № 1 (13).
  3. Internet Ethics / Edited by D. Langford. Houndmills etc., 2000.
  4. Баева Л. В. Информационная эпоха: метаморфозы классических ценностей. Астрахань: Издательский дом «Астраханский университет», 2008.
  5. Грачев Г. В. Личность и общество: информационно-психологическая безопасность и психологическая защита. М.: ПЕР СЭ, 2003.
  6. Информационные вызовы национальной и международной безопасности / Под ред. А. В. Федорова, В. Н. Цыгичко. М.: ПИР-Центр, 2001.
  7. Финн В. К. К структурной когнитологии: феноменология сознания с точки зрения искусственного интеллекта // Вопросы философии. 2009. № 1.

*Г. В. Фролов*

## ТИПИЗАЦИЯ ПРОЕКТНЫХ И ПРИКЛАДНЫХ РЕШЕНИЙ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ РАЗРАБОТКЕ ЗАЩИЩЕННЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Информационные технологии (ИТ) стали неотъемлемой частью повседневной жизни. На их основе удовлетворяются базовые потребности государства, бизнеса и гражданского общества по формированию, распространению, накоплению и потреблению информации.

ИТ эффективны тогда, когда они соответствуют потребностям текущего времени. Быстро изменяющиеся методы работы, появление на рынке новых ИТ-продуктов обуславливают потребность в создании новых и постоянной модификации и адаптации эксплуатирующихся информационных систем.

Для реализации новых общественных потребностей созданы высокоэффективные средства создания и развития ИТ. В частности, все большее развитие получает практика использования типовых решений, которые облегчают процесс разработки ИТ и снижают временные затраты.

В то же время практические подходы к разработке подсистем безопасности современных ИТ принципиально не изменились за последние десятилетия.

До недавнего времени практика разработки систем безопасности ИТ основывалась на нормативно-методологической базе, образованной Руководящими документами Гостехкомиссии России [1–5], которые были приняты в 90-х годах прошлого столетия. По мнению ряда авторов, они отражают «военный» подход к вопросу защиты информации, направленный на обеспечение ее конфиденциальности.

Анализ данных документов позволяет утверждать, что лежащий в их основе подход к разработке систем безопасности ИТ содержит элементы типизации проектных и прикладных решений в области защиты информации. В основе типизации лежит понятие «класс защищенности». Группировка ИТ по различным классам осуществляется на основании определяющих признаков, к которым относятся:

- наличие в ИТ информации различного уровня конфиденциальности;
- уровень полномочий субъектов доступа ИТ на доступ к конфиденциальной информации;
- режим обработки данных в ИТ — коллективный или индивидуальный.

На основании этих признаков выделены три типа ИТ:

- ИТ, в которых работает один пользователь, допущенный ко всей информации, размещенной на носителях одного уровня конфиденциальности;

