УДК 316.4
ББК 66

ПОНЯТИЕ И ХАРАКТЕРИСТИКА ИНФОРМАЦИОННЫХ РИСКОВ, ОПАСНОСТЕЙ И УГРОЗ В СОВРЕМЕННОМ ПОСТИНДУСТРИАЛЬНОМ ОБЩЕСТВЕ

А.А. Марков

Настоящая статья посвящена исследованию информационных рисков, опасностей и угроз на современном этапе развития цивилизации, в том числе – российского общества. В статье дается последовательная характеристика наиболее распространенных видов данных информационных понятий, деструктивных в отношении интересов личности и общества в информационной сфере.

Ключевые слова: *информационные риски, информационные опасности, информационные угрозы, интересы личности.*

Стратегия выживания человека на основе решения глобальных проблем современности должна вывести народы на новые рубежи цивилизованного развития [11]. Одной из таких проблем является создание и функционирование глобального информационного пространства, которое, помимо очевидных преимуществ и благ для человечества, предопределяет и наличие глобальных информационных угроз, опасностей и рисков.

Особенность глобальных информационных угроз заключается в том, что их источники не направлены на конкретного субъекта информационного мирового пространства, то есть не проецируются на личность и общество определенного государства, но охватывают их, так сказать, в совокупности. Иначе говоря, глобальные информационные риски, опасности и угрозы носят обезличенный характер и касаются всех, но понятие «все» не имеет конкретного адресата. Так, глобальную информационную угрозу может содержать в себе ослабление в целом контроля цивилизации (в том числе и из-за отсутствия элементарной договоренности между государствами) над множащимися информационными потоками и развитием информационно-коммуникационных технологий.

Например, наднациональной, то есть глобальной угрозой для мировой социальной нравственности является легальный и практически ненаказуемый (за исключением эпизодических случаев, лишь подчеркивающих нерешенность проблемы) поток порнографических сайтов, а в последнее время – выросшее количество сайтов детской порнографии, инцеста и пр. в сети Интернет. В техническом аспекте информационной безопасности такую угрозу может представлять некий глобальный компьютерный вирус. Непонятно, к примеру, какую степень информационной угрозы будет представлять та же нейрореволюция, когда станет возможным архивировать в компьютере данные человеческого мозга: насколько это будет способствовать прогрессу человечества или же приближать его к катастрофе, потому что подобная революция способна создавать не только гениев, но и киборгов. А учитывая, что всякое научно-техническое достижение или новшество в первую очередь арендуется для военных нужд, возможный расклад вполне очевиден со всеми вытекающими последствиями.

Иной характер представляют внешние информационные опасности и угрозы. В отличие от глобальных аналогов, имеющих достаточно космополитический характер, внешние информационные опасности и угрозы имеют конкретную направленность. Внешняя

информационная угроза умышленно направлена на информационную безопасность субъекта. Так, объектом угроз информационной безопасности организации выступают сведения о составе, состоянии и деятельности объекта защиты (персонала, материальных и финансовых ценностей, информационных ресурсов). Угрозы информации выражаются в нарушении ее целостности, конфиденциальности, полноты и доступности. Источниками угроз выступают конкуренты, преступники, коррупционеры, административно-управленческие органы. Источники угроз преследуют при этом следующие цели: ознакомление с охраняемыми сведениями, их модификация в корыстных целях и уничтожение для нанесения прямого материального ущерба. Неправомерное овладение конфиденциальной информацией возможно путем ее разглашения источниками сведений, утечки информации через технические средства и несанкционированного доступа к охраняемым сведениям [8].

Прежде чем проанализировать воздействие глобальных и внешних информационных рисков, опасностей и угроз на информационную безопасность нынешнего отечественного социума, исследуем понятия и сущность информационных рисков, опасностей и, собственно говоря, угроз как самостоятельных определений. Это будет способствовать правильному осмыслению построения современной эффективной системы обеспечения информационной безопасности российского общества.

Рассматривая современную систему и основные направления обеспечения информационной безопасности российского социума, определяя ресурсы и технологии данного обеспечения, мы обязаны исходить из современного анализа рисков, опасностей и угроз информационного характера, воздействующих на интересы личности и общества (а также и государства, если иметь в виду деструктивный характер этих угроз государственного уровня, негативно воздействующий на социальное самочувствие социума), в том числе исследовать сущность и классификацию этих рисков и угроз. Образно выражаясь, требуется досконально знать оружие противника, чтобы подготовиться к успешному сражению с ним.

Исследование концепции и системы обеспечения информационной безопасности нуждается в определении понятийного аппарата, содержания и классификации информационных опасностей и угроз, а также информационных рисков для личности, общества и государства. Понимание этих категорий позволяет сформулировать эффективные варианты решения в плане практической реализации противодействия указанным категориям. При этом следует учесть, что по мере развития цивилизации и общественных отношений в социуме традиционное понимание того, что в целом система безопасности должна строиться на такой базовой категории, как имеющийся или потенциальный (внешний и внутренний) противник, победа над которым и обеспечивает эту безопасность, представляется однобоким. Современное исследование проблем безопасности, включая и информационную безопасность, должно включать не только персонифицированные опасности, угрозы и риски, но и осмысление их источника и характера.

Относительно недавно данные понятия практически не изучались в отечественной и зарубежной социологией и другими гуманитарными науками, на что указывает Я.А. Маргулян [12, с. 74]. Однако с актуализацией исследований о современной природе и сущности безопасности как неотъемлемого явления и в значительной степени гаранта общечеловеческой жизнедеятельности ситуация изменилась. Применительно к информационной безопасности рассмотрим сущностные понятия «информационный риск», «информационная опасность», «информационная угроза» не только как обобщенные явления, но и через спектр их определенных направлений, что позволяет выделить и конституировать их разновидности.

Информационный риск. Риск как понятие представляет собой возникновение ситуации, характеризующейся неопределенностью результата, вероятным или обязательным наличием неблагоприятных последствий. Риск предполагает неуверенность либо невозможность получения достоверного знания о благоприятном исходе в заданных внешних обстоятельствах. В.В. Глушенко определяет риск как действующий/развивающийся фактор процесса, обладающий потенциалом негативного влияния на ход процесса [4].

Существует достаточное количество определений риска, которые могут быть воспроизведены в различных ситуационных контекстах и различными особенностями применений. Очевидно, что риск (мера риска) в определенном смысле пропорционален как ожидаемым потерям, которые могут быть причинены рисковым событием, так и вероятности этого события. Различия в определениях риска зависят от величины потерь, их оценки и измерения. Если потери оказываются фиксированными, оценка риска фокусируется только на вероятности события, возможных его последствий и связанных с ними обстоятельств. Можно выделить две разновидности риска: теоретический риск и эффективный риск. Эти две точки зрения непрерывно конфликтуют в социальных, гуманитарных и политических науках. В последние годы в связи с появлением нового направления теории вероятностей – эвентологии – возникло понятие эвентологического риска, которое можно рассматривать как первую серьезную попытку объединить в одном понятии и теоретический, и эффективный риск [16].

В информационной безопасности риск определяется как функция трех переменных величин: вероятность существования информационной угрозы; вероятность существования незащищенности; потенциальное воздействие. Если любая из этих переменных приближается к нулю, полный риск приближается к нулю. На наш взгляд, информационный риск представляет собой определенные и осознанные действия субъекта в информационной сфере, предполагающие возникновение возможных негативных последствий. Примером таких рисков может служить PR-компания/PR-акция, реклама, предвыборная политическая пропаганда, продвижение продукта коммерческой компании на рынок, информационная атака/война в отношении конкурента (противника), внесение в адресные базы важных конфиденциальных данных, работа с новыми, малопроверенннными техническими средствами либо работа на компьютере (или запуск сервера) без надлежащей антивирусной программы, и т. д. Заложенные в таком случае информационные риски предполагают наличие осознанности своих действий субъектом, который осознает вероятность возникновения негативных последствий на определенной стадии или по окончании реализации своих действий. В качестве таковых последствий могут выступать контрдействия конкурентов, несоответствие затрат на производство PR или рекламного продукта полученному доходу, неподготовленность общественного мнения к восприятию информационных поводов (идей) субъекта, хакерские или вирусные «инъекции» в компьютерную систему, наконец, результаты свойственного российскому менталитету расчета на «авось» (например, возможное отключение электричества при проведении срочной компьютерной работы без постоянного сохранения параметров этой работы) и т. д. В настоящее время информационные риски уже являются не только предметом изучения, но и защиты, в том числе страховой. Например, с развитием IT-технологий услуга по страхованию информационных рисков становится востребованной и в России. Первой конкретной страховой программой стал совместный проект компании «ИнфоОборона» и ОСАО «Ингосстрах». Начиная с июня 2008 г. компании, работающие на территории России, получают возможность оформить страхование информационных рисков, которое включает в себя: страхование имущества страхователя от огня и других опасностей, включая злоумышленные действия третьих лиц; страхование электронного оборудования от специфических рисков, связанных с энергоснабжением; страхование гражданской ответственности; страхование информационных систем, баз данных; страхование убытков от перерыва в деятельности и др. [9].

Таким образом, информационный риск является проявлением и следствием добровольной и осознанной деятельности самого субъекта в информационной сфере. Кроме того, информационный риск может стать причиной появления информационной опасности.

Информационная опасность. В наиболее обобщенном виде опасность представляет собой совокупность вероятных или реально действующих факторов, процессов и явлений, которые могут оказать деструктивное воздействие на объекты и субъекты, подвергающиеся опасному посягательству. Опасность предполагает возможность возникновения обстоятельств, при которых материя, поле,

информация или их сочетание могут таким образом повлиять на сложную систему, что это приведет к ухудшению или невозможности ее функционирования и развития. В зависимости от своей природы, количественной и качественной характеристик, продолжительности действия опасность способна оказать значительное отрицательное воздействие на субъекты опасности. Источники опасностей бывают как естественными (землетрясения, наводнения, пожары, глобальное потепление и др.), так и антропогенными (войны, конфликты, экологическая, техногенная, промышленная и др. опасности).

Кроме того, существуют источники так называемой повышенной опасности антропогенного характера, квалификация которых находит отражение в правовых нормах, в частности в Гражданском праве. Так, действующий Гражданский кодекс Российской Федерации указывает, что юридические лица и граждане, деятельность которых связана с повышенной опасностью для окружающих (использование транспортных средств, механизмов, электрической энергии высокого напряжения, атомной энергии, взрывчатых веществ, сильнодействующих ядов и т. п.; осуществление строительной и иной связанной с нею деятельности и др.), обязаны возместить вред, причиненный источником повышенной опасности, если не докажут, что вред возник вследствие непреодолимой силы или умысла потерпевшего [6]. В п. 17 Постановления Пленума Верховного суда РФ от 28 апреля 1994 г. дается следующее определение источника повышенной опасности: источником повышенной опасности надлежит признать любую деятельность, осуществление которой создает повышенную вероятность причинения вреда из-за невозможности полного контроля за ней со стороны человека, а также деятельность по использованию, транспортировке, хранению предметов, веществ и иных объектов производственного назначения, обладающих такими же свойствами [13].

Из приведенных определений видно, что отечественный законодатель, устанавливая основания и пределы ответственности за вред, причиненный источником повышенной опасности, традиционно оперирует двумя близкими, но не тождественными понятиями: а) деятельность, связанная с повышенной опасностью для окружающих; б) источник повышенной опасности.

В праве существуют две позиции определения источника анализируемого понятия. Первая позиция: под источником повышенной опасности понимается деятельность, которая, будучи связана с использованием определенных вещей, не поддается непрерывному и всеобъемлющему контролю человека, вследствие чего обусловливает высокую степень вероятности причинения вреда. Согласно второй позиции, под источником повышенной опасности понимаются свойства вещей или силы природы, которые при достигнутом уровне развития техники не поддаются полностью контролю человека и, не подчиняясь полностью контролю, создают высокую степень вероятности причинения вреда жизни или здоровью человека либо материальным благам.

Опасности характеризуются потенциалом, качеством, временем существования или воздействия на человека, вероятностью появления, размерами зоны действия. Потенциал проявляется с количественной стороны (например, уровень шума, запыленность воздуха, напряжение электрического тока). Качество отражает его специфические особенности, влияющие на организм человека (например, частотный состав шума, дисперсность пыли, род электрического тока). Мерой опасности может выступать и число пострадавших. Другой мерой опасности может быть и приносимый ее реализацией ущерб (например, ущерб для окружающей среды, который только частично может быть измерен экономически, в основном через затраты на ликвидацию последствий).

К числу опасностей многие исследователи справедливо относят целеустремленные враждебные намерения и действия одних субъектов против других, включая и вредные последствия этих действий и намерений, а также таковые последствия в результате некомпетентности, ошибок, халатности и т. д. [14, с. 11–15].

Информационная опасность, на наш взгляд, заключается как в действиях самого субъекта информационной сферы, своими непрофессиональными, самонадеянными, ошибочными действиями или в результате информационного рис-

ка нанесшего вред собственным интересам в данной сфере (внутренний аспект), так и в спонтанном (неумышленном) или преднамеренном нанесении вреда интересам субъекта в информационной сфере внешней стороной (внешний аспект).

Здесь важно учесть, что субъект информационной среды никогда не ставит цели нанесения вреда своим информационными правам и интересам, предполагая потенциально или реально возникающую информационную опасность (риск) предусмотреть или преодолеть. Способность подобного преодоления всецело относится к личностным характеристикам субъекта. Вместе с тем причиненный вред и размер ущерба в результате реализации информационной опасности по вине самого субъекта в количественной и качественной оценках может быть различным: от незначительного до огромного (например, самонадеянность в работе с банком данных в компьютерной системе организации, которая привела к невозвратному уничтожению важнейших файлов). Однако надо признать, что субъект информационной среды наносит ущерб своим информационным интересам неосознанно, неумышленно.

Информационная опасность, исходящая от внешней стороны, также может быть непредвиденной, то есть спонтанной, когда потенциальное или реализуемое действие (бездействие) этой стороны не содержат в себе умысла. Таковой может быть публикация в СМИ материала, не согласованного с источником информации по вине журналиста, посчитавшего, что он сам компетентен в освещаемой им теме; либо неисполненное по халатности обещание передать важное сообщение в оговоренные сроки; либо это могут быть случайные действия провайдера сети, осуществившего несанкционированный доступ на сайт организации, и т. д.

И информационная опасность, исходящая от внешней стороны, может быть преднамеренной, спланированной с целью нанесение вреда субъекту информационной среды. В таком случае налицо умысел в реализации подобных действий: внешняя сторона специально организует (создает) информационную опасность, желая наступления вредных последствий для определенного субъекта. Здесь можно привести в пример фальсифицированную и клеветническую информацию в адрес личности или организации с целью их дискредитации.

Тем не менее, на наш взгляд, информационная опасность более всего представляет собой побуждение к определенному действию (бездействию), которое, в принципе, можно предвидеть, а значит, своевременно предотвратить или минимизировать вред и ущерб от его реализации и тем самым обеспечить защиту интересов субъекта информационной сферы.

Информационная угроза. В общем понятии угроза представляет собой намерение реализовать вероятную опасность. Само понятие «угроза» не имеет четкого единого определения и многими авторами трактуется по-разному. Например, угроза определяется как «высказанное в любой форме намерение нанести физический, материальный иди иной вред общественным и личным интересам» [15]. Ряд авторов считают, что угроза – это «совокупность факторов и условий, представляющих опасность жизненно важным интересам личности, общества и государства» [3, с. 45].

Другие полагают, что угроза – это «наиболее конкретная и непосредственная форма опасности, создаваемая целенаправленной деятельностью откровенно враждебных сил» [2, с. 91].

В.В. Барабин представляет угрозу как актуализированную форму опасности в процессе ее превращения из возможности в действительность, субъективированную готовность одних людей причинить ущерб другим [1, с. 33].

Последняя позиция нам представляется наиболее убедительным определением понятия угрозы. На наш взгляд, если мы рассматриваем опасность как побуждение к действию, то, собственно говоря, угроза означает непосредственную готовность осуществления такой опасности. Здесь важно понять грань между терминами «намерение» и «готовность». Намерение представляет собой некую подготовительную фазу для реализации соответствующих целей. Готовность предполагает, что данная фаза окончена и следующей станет непосредственное действие. Образно го-

воря, угрозу можно охарактеризовать как последнее предупреждение, за которым и последует само действие.

Информационная угроза, по сути, представляет собой умысел с целью намеренного нанесения вреда субъекту информационной сферы. В отличие от информационного риска и частично информационной опасности, информационная угроза направлена против интересов субъекта в данной сфере. А учитывая нынешнее развитие информационно-коммуникационных технологий и информационных ресурсов, возрастающее и неуклонное влияние информации на жизнедеятельность личности, общества и государства, а также происходящие процессы глобализации человечества, можно утверждать, что информационные угрозы способны не только воздействовать на информационную безопасность, но также в тех или иных параметрах оказывать деструктивное влияние на национальную, экономическую, экологическую, социальную и ряд других видов безопасности.

Например, угрозы информационной безопасности Сетей связи общего пользования (ССОП) Министерство Российской Федерации по связи и информатизации видит в возможном воздействии нарушителя информационной безопасности на информационную сферу ССОП, непредотвращение, необнаружение и неликвидация последствий которого средствами ССОП может привести к ухудшению заданного уровня качества службы, или к ухудшению заданных качественных характеристик функционирования ССОП, и, как следствие, к нанесению ущерба государству, пользователю или оператору связи ССОП [10].

Таким образом, квалифицируя исследованные выше информационные риски, опасности и угрозы, можно сделать вывод: информационные риски и отчасти информационные опасности (без наличия умысла) представляют собой потенциально вредные намерения и действия, способные нанести определенный ущерб субъектам информационной сферы. Информационные угрозы являют реальную готовность нанесения вреда и желание наступления негативных последствий для субъектов информационной и иных сфер жизнедеятельности личности, общества и государства. При этом следует уточнить: информационные риски и опасности могут стать причиной появления информационной угрозы безотносительно того, умышленны они или нет.

Совершенно очевидно, что именно информационные угрозы представляют наибольшую проблему в обеспечении информационной безопасности субъекта, так как содержат в себе качественные квалифицирующие признаки повышенной потенциальной и реальной деструкции. В то же время анализ имеющейся литературы и иной информации по данной теме свидетельствует, что лишь информационные угрозы представляют в общем понятийном смысле ту категорию, которая прямо влияет на информационную безопасность. Допускаем, что в определение «информационная угроза» многими авторами вкладывается и суть определений «информационная опасность» и «информационный риск», но отдельно ими не рассматривается, чтобы не усложнять общую конструкцию, либо по причине относительной малозначительности воздействия на информационную безопасность. Таким образом, мы полагаем, что следует квалифицировать все эти определения, и в дальнейшем, по мере совершенствования информационного общества и его информационной безопасности, эти определения станут самостоятельными понятиями и будут анализироваться как самостоятельные категории. На сегодняшний день достаточно ограничиться характеристикой информационных угроз.

Информационные угрозы могут быть преддверием последующих действий, которые выражаются в таких формах, как информационная война, информационная атака, информационный шантаж, хакерство, нарушение или вывод из строя технических и информационно-коммуникационных систем, несанкционированный доступ в компьютерные системы собственника или владельца информации, шпионаж, публичное разглашение секретных и конфиденциальных сведений, нарушение права на частную жизнь, кража персональных данных, фальсификация данных, умышленная негативная информация с целью нанесения ущерба имиджу личности или организации, клевета, фальсификация и уничижение национальных и государственных институтов, приоритетов, святынь, проектов, идеологии и др., пропаганда асоциальных и аморальных установок и

норм, разрушение духовно-нравственных ценностей социума и т. д.

Виды угроз информационной безопасности Российской Федерации обстоятельно представлены в ее Доктрине информационной безопасности [7].

СПИСОК ЛИТЕРАТУРЫ

1. Барабин, В. В. Военно-политическая деятельность государства в системе национальной безопасности / В. В. Барабин. – М. : Изд-во МО РФ, 1998. – 124 с.
2. Безопасность // Информационный сборник фонда национальной и международной безопасности. – 1994. – № 3 (19). – С. 91.
3. Ващекин, Н. П. Безопасность и устойчивое развитие России / Н. П. Ващекин, М. И. Дэлиев, А. Д. Урсул. – М. : ИНФРА-М, 1998. – 112 с.
4. Глущенко, В. В. Введение в кризисологию. Финансовая кризисология. Антикризисное управление / В. В. Глущенко. – М. : ИП, 2008. – 88 с.
5. Глущенко, В. В. Риски инновационной и инвестиционной деятельности в условиях глобализации / В. В. Глущенко. – М. : НПЦ «Крылья», 2006. – 230 с.
6. Гражданский кодекс Российской Федерации. – М. : Право, 2006. – Ст. 1079.
7. Доктрина информационной безопасности Российской Федерации // Российская газета. – 2000. – 25 нояб. – № 227 (2591).
8. Защита информации в системе безопасности предприятия [Электронный ресурс]. – Электрон. текстовые дан. – Режим доступа: http://www.content-security.ru/articles/. – Дата обращения: 15.11.2009. – Загл. с экрана.
9. Компания «ИнфоОборона» и ОСАО «Ингосстрах» представляют новый продукт: страхование информационных рисков [Электронный ресурс]. – Электрон. текстовые дан. – Режим доступа: http://www.infooborona.ru/folder55.html. – Дата обращения: 13.10.2009. – Загл. с экрана.
10. Концепция информационной безопасности Сетей связи общего пользования Взаимоувязанной сети связи Российской Федерации [Электронный ресурс] / Министерство Российской Федерации по связи и информатизации. – Электрон. текстовые дан. – М., 2002. – Режим доступа: http://www.ifap.ru/. – Дата обращения: 11.09.2009. – Загл. с экрана.
11. Мальцев, В. А. Основы политологии / В. А. Мальцев. – М. : ИТРК, 2002. – 544 с.
12. Маргулян, Я. А. Система и способы обеспечения социальной безопасности : монография / Я. А. Маргулян. – СПб. : СПбВИТУ, 2000. – 240 с.
13. Постановление Пленума Верховногосуда РФ от 28 апреля 1994 г. № 3 «О судебной практике по делам о возмещении вреда, причиненного повреждением здоровья» // Бюллетень Верховного суда Российской Федерации. – 1994. – № 7.
14. Серебрянников, В. В. Безопасность России и армия / В. В. Серебрянников [и др.]. – М. : Изд-во МО РФ, 1995. – 204 с.
15. Советский энциклопедический словарь. – М. : БСЭ, 1990. – 1600 с.
16. Dirk Proske Catalogue of Risks – Natural, Technical, Social and Health Risks. – Springer, 2007. – 314 p.

THE NOTION AND CHARACTERISTICS OF INFORMATION RISKS, DANGERS AND THREATS IN THE MODERN POST-INDUSTRIAL SOCIETY

A.A. Markov

The present article is devoted to the research of information risks, dangers and threats at the current stage of the civilization development including the Russian society. Consecutive characteristic of the most well-known information concepts data types destructive towards personal and social interests in media is given.

Key words: *information risks, information dangers, information threats, interests of the person.*