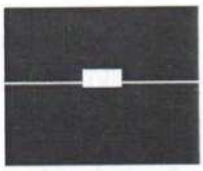

ПОРТФЕЛЬ РЕДАКЦИИ

БИТ

I.Yu. Alekseeva
Institute of Philosophy, Russian Academy of Sciences, 109240, Moscow, ul. Goncharnaya, 12, str. 1, DSc in Philosophy, Leading Research Fellow, e-mail: ialexeev@inbox.ru, ORCID iD 0000-0002-0514-8237

Information Security in the Context of Philosophy of Management

Keywords: information and psychological security, social system, philosophy of management, philosophy of complexity.

Building a culture of information security involves consideration of problems of management in society. Ideas and approaches developed in philosophy of management are relevant to studies in problems of information security in broader methodological and social context. The article focuses on problems of information and psychological security in social systems. The author considers disorienting signs and signals as information threat to security of persons and societies. The author argues that management ideology of pseudo-economical reductionism makes distortion at the level of values and priorities of the system. This ideology exalts competitiveness to the detriment of the systems' viability. Philosophy of complexity (better known as «philosophy of complex systems») embraces new visions for methodology of management in XXI century. «Observer of complexity» and «complexity of observer of complexity» phenomena are central in this context. The problem of appropriate language for system self-description is of critical importance. This language is necessary for substantive production of intellectual tools for problems solving and decision making; refusal to produce such tools is fraught with decrease of information security level.

И.Ю. Алексеева
Институт философии Российской академии наук, 109240, г. Москва, ул. Гончарная, д.12, с.1, доктор философских наук, ведущий научный сотрудник, e-mail: ialexeev@inbox.ru, ORCID iD 0000-0002-0514-823

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В КОНТЕКСТЕ ФИЛОСОФИИ УПРАВЛЕНИЯ[1]

Ключевые слова: Информационно-психологическая безопасность, социальная система, философия управления, философия сложности.

[1] Работа выполнена при финансовой поддержке РГНФ. Проект № 15-03-00248: Проведение научных исследований по направлению «Формирование в обществе культуры информационной безопасности».

Проблемы формирования культуры информационной безопасности в обществе тесно связаны с проблемами управления. Идеи и подходы, развиваемые в современной философии управления, способствуют осмыслению феномена информационной безопасности в широком методологическом и социальном контексте. В статье рассматриваются проблемы защиты социальных систем от информационных угроз, связанных с усилением роли дезориентирующих тенденций в управлении. Особое внимание уделено отрицательным последствиям псевдоэкономического редукционизма в управленческой идеологии и практике. Редукционизм такого рода искажает информационно-ориентировочную основу управления социальной системой на уровне, где определяются основные ценности и приоритеты. В результате стремление к узко понимаемой конкурентоспособности ставит под вопрос саму жизнеспособность системы. Новые перспективы для методологии управления открывает формирующаяся в XXI веке философия сложности (направление, более известное как «философия сложных систем»). В этом контексте особое значение приобретают феномен «наблюдателя сложности» и необходимость принимать во внимание «сложность наблюдателя сложности». В статье показана зависимость качества управления от наличия языковых средств, необходимых для описания систем. Отказ от собственного производства интеллектуального обеспечения решений оценивается как фактор понижения уровня информационной безопасности социума.

Проблемы информационной безопасности тесно связаны с проблемами управления. Это верно как в отношении аспектов информационной безопасности, изучаемых инженерно-техническими и физико-математическими науками, так и в отношении вопросов, обсуждаемых в философии и других гуманитарных областях.

Здесь, как и в ранее выполненной работе [1], мы исходим из предложенного А.А. Малюком определения информационной безопасности как «такого состояния рассматриваемой системы, при котором она, с одной стороны, способна противостоять дестабилизирующему воздействию внешних и внутренних информационных угроз, а с другой – ее функционирование не создает угроз для элементов самой системы и внешней среды» [7, с. 12]. К информационной безопасности относят вопросы защиты информации от несанкционированный модификации, искажения, уничтожения, злонамеренного использования, вопросы обеспечения должного качества информации, а также способы защиты людей и технических систем от разрушающего воздействия информации. Таким образом, проблематика информационной безопасности охватывает не только технические, но и биологические, социальные и биосоциальные системы. Полное отсутствие как внешних, так и внутренних угроз достижимо только в идеальной ситуации. На деле же обеспечение безопасности требует мер, направленных на защиту от имеющихся угроз и предотвращение возникновения новых.

Идеи и подходы философии управления, развиваемые в работах В.С. Диева [5, 6], В.М. Розина и Л.Г. Голубковой [3, 10] М. Дибена и С. Ширда [12], Л. Фролунда и М. Зитхена [14] способствуют осмыслению феномена информационной безопасности и вопросов формирования культуры информационной безопасности в широком методологическом и социальном контексте. А упомянутые вопросы, в свою очередь, дают импульс обсуждению в рамках философии управления условий и критериев рациональности стратегий и методов с учетом задач обеспечения жизнеспособности управляемых (и управляющих) систем и подсистем.

Управление в самом общем смысле как имеющее место в системах разной природы, включая технические, биологические и социальные, предполагает функции поддержания и (или) улучшения системных характеристик в процессе воздействия на объекты внутри системы и вне ее. Управление в социальных системах осуществляется

субъектами целенаправленной деятельности, рамки и характер которой во многом определяются условиями безопасности системы в целом, ее подсистем и элементов.

Не будет преувеличением сказать, что слово «эффективность» используется сегодня как ключевое в характеристике и оценке управления. Однако вопрос о том, что такое эффективность и каковы способы ее определения, отнюдь не тривиален. Под эффективностью понимают и достижение наилучших результатов с наименьшими затратами ресурсов (в частности, выпуск наибольшего количества товаров в расчете на единицу затрат), и способность в пределах заданного времени решать задачи и выполнять планы любого характера, и степень соответствия системы своему функциональному назначению, целям, для которых она создана.

Современная практика управления в социальных системах свидетельствует об усилении редукционистских тенденций, заменяющих общие (неизбежно носящие качественный характер) представления о целях и принципах работы систем якобы более современными количественными методами оценки эффективности управляющих и управляемых подсистем. При этом формируются новые идеалы эффективности, ориентирующие на уподобление любого вида деятельности производству товаров, а также наиболее выгодной продаже товаров и получению процентов по вкладам и акциям. Подобные тенденции позволяют упростить картины управляемых объектов, которые слишком сложны для «эффективных менеджеров», имеющих весьма поверхностные представления о сферах своей ответственности. В таком контексте стремление к созданию максимальных удобств для субъекта управления порождает дезориентирующие знаки – особый вид информационных угроз как управляемому объекту, так и системе в целом. Погоня за конкурентоспособностью, измеряемой очками и баллами, выступающими в роли подобий товаров и денежных единиц, способна поставить под вопрос саму жизнеспособность системы.

Дезориентирующие знаки вызывают изменения в моделях мира, имеющихся у самообучающихся систем, искажают цели и правила поведения, меняют фактологическую основу принятия решений, влияя на восприятие и оценку фактов [8, 15, 17]. А.В. Раскин справедливо отмечает, что такую сложную информационную систему, как человек, можно «вывести из строя», активизируя определенные желания и мысли, провоцируя поступки, ведущие к саморазрушению [9]. Добавим к сказанному, что подобным образом могут «выводиться из строя» и социальные системы, причем не только в результате действий, имеющих целью разрушение систем, но и вследствие деятельности, субъективно направленной на совершенствование этих систем, улучшение их характеристик и т.д.

Развитие информационно-коммуникационных технологий ведет к тому, что человек получает всё больше семантической (смысловой) информации через технические каналы связи, а не из личного опыта и непосредственного общения. При этом существенная часть как текстовой, так и аудио- и видеоинформации подготавливается и передается в рамках специально предназначенных для этого структур и организаций, широко использующих манипулятивные информационно-психологические воздействия. В таких условиях проблемы социально-психологической безопасности всё чаще выглядят как проблемы информационно-психологические.

Информационно-психологическая безопасность характеризуется уровнем психологического потенциала (личности, коллектива, социума), который не должен опускаться ниже допустимых пределов. Г.М. Зараковский подчеркивает, что именно психологический потенциал как интегральная характеристика индивида позволяет последнему осуществлять продуктивную жизнедеятельность. Соответственно, продуктивная жизнедеятельность социума немыслима без коллективного психологического потен-

циала, который зависит не только от психологических свойств отдельных людей, но и от структурно-функциональных характеристик организаций и общественного организма в целом. Продуктивной жизнедеятельности присущи такие черты, как устойчивость, способность удовлетворять биологические и духовные потребности людей, обеспечивать растущий уровень независимости общества от неблагоприятных средовых условий [11, с. 6–7]. Этого невозможно достичь без развития технологий, однако такое развитие несет с собой и новые риски.

Условием информационно-психологической безопасности является и наличие адекватной информационно-ориентировочной основы поведения субъекта (индивида, организации, социума). С этих позиций Г.В. Грачёв правомерно рассматривает в качестве угроз безопасности информационные факторы, которые препятствуют формированию информационно-ориентировочной основы, необходимой для деятельности людей, адекватного социального поведения человека и успешного функционирования общества [4, с. 145]. Обеспечение информационно-психологической безопасности предполагает защищенность сознания и психики человека (как и общественного сознания) от информационных угроз, которые могут быть результатом целенаправленных разрушительных воздействий, но могут возникать и вследствие взаимодействия разнообразных тенденций и процессов в современной информационной среде.

В общем случае знание природы и основных приемов манипулятивных информационно-психологических воздействий повышает возможности сопротивления таким воздействиям. Вместе с тем уровень информационно-психологической защищенности субъекта зависит от таких факторов, как самостоятельность мышления, способность анализировать информацию, осознавать собственные интересы, создавать и реализовывать планы. И высокий психологический потенциал, и адекватная информационно-ориентировочная основа поведения и деятельности – необходимые условия информационно-психологической безопасности личности и общества. Однако концентрация внимания человека на информации, подобранной таким образом, чтобы создать у данного человека негативное представление о себе самом (даже если такая информация достоверна) способны привести к понижению психологического потенциала до опасно низкого уровня. Аналогичное происходит и с социумом. Оправданно ли в данном случае утверждать, что задачи обеспечения адекватной информационно-ориентировочной основы поведения вступают в противоречие с задачами поддержания необходимого психологического потенциала? Подобный вывод был бы чересчур поспешным, поскольку такая информационно-ориентировочная основа представляет собой не просто набор каких-либо фактов (односторонне характеризующих ситуацию), а достаточно сложную картину человека и общества с их настоящим, прошлым и возможным будущим. Информация, используемая в создании такой картины, в идеале должна быть достоверной, объективной, всестороннее характеризующей ситуацию, и при этом соответствующей целям выживания и развития социального субъекта (индивидуального или коллективного). Это следует принимать во внимание, разрабатывая стратегию управления в социальной системе. Под философией управления мы понимаем как совокупность лежащих в основе практической управленческой деятельности мировоззренческих и методологических установок (имеющих более или менее осознанный характер), так и формирующийся особый раздел, или направление в философских исследованиях. Философия управления в последнем смысле, изучая и оценивая ориентиры и установки управленческой практики, стремится раскрыть возможности определенных методологических подходов в выработке адекватной ориентировочной основы управления. В последние годы в этом контексте правомерно упоминаются подходы, разрабатываемые

в рамках философии сложности – направления, более известного как «философия сложных систем», связанная с именем С. Хукера [16].

В.И. Аршинов выдвигает на первый план феномен «наблюдателя сложности», подчеркивая при этом необходимость принимать во внимание «сложность наблюдателя сложности» [2, с. 58]. Серьезное влияние на философию сложности оказывают идеи синергетики и «кибернетики второго порядка». Как известно, приверженцы последней называют «первопорядковой» кибернетику, изучающую наблюдаемые системы, а «второпорядковой» – кибернетику, которая изучает наблюдающие системы. «Первопорядковая обусловленность» предполагает, что поведение наблюдателя, включенного в систему, определяется целями системы, а «второпорядковая» – что наблюдатель, включаясь в систему, руководствуется собственными целями [13].

Социальная система в процессах познания и самопознания является «наблюдателем» собственной сложности и сложности других систем (в том числе систем, в которые включена исходная). От формирующихся в этих процессах «моделей мира» зависит постановка задач управляющими подсистемами, определение путей решения и критериев эффективности, а также поведение и жизнеспособность системы в целом. Упрощение реальности в ходе познания неизбежно, однако неадекватность базовых моделей, порождаемых в погоне за односторонне понятой эффективностью, не компенсируется применением передовых технических средств, позволяющих собирать и обрабатывать огромные объемы данных.

Исследователи относят проблему языка описания объектов и процессов управления к числу важнейших для современного управленческого знания. В.М. Розин и Л.Г. Голубкова правомерно обращают внимание на то обстоятельство, что в нашей стране отказ от советских методов, неприменимых в условиях нового российского капитализма, сопровождался некритическим заимствованием инженерного подхода к организации, характерного для западных (прежде всего американских) моделей управления. Применение этих моделей на практике сталкивается с серьезными трудностями, а успехи, достигнутые в результате собственных «находок», не могут быть переведены в «отчуждаемую» методику, поскольку для таковой нет соответствующих языковых средств. Складывается ситуация, когда положительный опыт имеется, его передача необходима, однако невозможна вследствие «бессловесности» отечественной управленческой культуры, словарь которой едва ли не исчерпывается скудным менеджерским «новоязом». «Задачи современного управления, – пишут В.М. Розин и Л.Г. Голубкова, – требуют от руководителей умения работать с картинами мира сотрудников и партнеров, а это при отсутствии соответствующих навыков и разработанного языка практически невозможно» [10, с. 33]. К сказанному мы можем добавить, что в условиях распространения псевдоэкономических подходов на все сферы жизни общества и человека перспектива затраты каких-либо ресурсов на создание подобных языков может отвергаться «с порога» как не вписывающаяся в рамки узкого понимания рациональности и эффективности. С таких позиций насыщение русского «новояза» кальками английских слов и выражений (без учета многозначности этих слов в языке заимствования!) выглядит экономичным и эффективным решением вопроса, создает иллюзию движения к «мировому уровню», а разговоры о несоответствии полученных конструкций картинам мира и ценностям людей воспринимаются как отвлекающие от насущных задач повышения конкурентоспособности.

Современное общество не может существовать, не получая информации и знаний в процессах взаимодействия с другими обществами. Однако позиции и степень влияния в глобальной инфосфере у разных участников коммуникации различны. В процессе взаимодействия коммуникантов-социумов происходит перенесение правил, установок

и ценностей от более сильных коммуникантов к более слабым. Кроме того, последние нередко действуют по рецептам, которые целенаправленно созданы для них представителями сильного коммуниканта. Порой использование таких рецептов выглядит целесообразным, поскольку избавляет от затрат времени и средств на собственное производство интеллектуального обеспечения решений, открывая возможности импорта готовых инструментов и инструкций по их применению. Однако восприятие и эффекты импортируемых установок существенным образом зависят от условий, имеющихся в социуме-реципиенте. Возникают и проблемы с качеством рецептов, предназначенных для принимающего социума, с наличием у их авторов достаточных знаний и заинтересованности в благополучии «пациента». Использование моделей и принципов работы, не учитывающих содержания и свойств принимающей системы, может вести к разрушению жизненно важных для нее элементов и подсистем. В таком контексте правомерно вести речь об информационных (в широком смысле слова [20]) угрозах безопасности подсистем и системы в целом, когда собственно информационно-технологический характер имеет лишь часть таких угроз.

Без самостоятельной творческой работы, позволяющей учитывать сложность человека и мира, осознавать ценности, определять приоритеты, ставить цели и конструировать механизмы их достижения невозможно создание адекватных информационно-ориентировочных основ функционирования социальной системы.

СПИСОК ЛИТЕРАТУРЫ:

1. Алексеев А.П., Алексеева И.Ю. Информационная война в информационном обществе // Вопросы философии. 2016. № 11. С. 5–14.
2. Аршинов В.И. Синергетика встречается со сложностью // Синергетическая парадигма. Синергетика инновационной сложности. М., 2011. С. 47–65.
3. Голубкова Л.Г., Розин В.М. Философия управления. Йошкар-Ола: МарГТУ, 2010.
4. Грачев Г.В. Личность и общество: информационно-психологическая безопасность и психологическая защита. М.: ПЕР СЭ, 2003.
5. Диев В.С. Рациональные решения: критерии, модели, парадоксы // Вопросы философии. 2013. № 8. С. 4–11.
6. Диев В.С. Управление. Философия. Общество // Вопросы философии. 2010. № 8. С. 35–41.
7. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. М.: Горячая линия – Телеком, 2004.
8. Минаев В.А., Дворянкин С.В. Обоснование и описание модели динамики информационно-психологических воздействий деструктивного характера в социальных сетях // Безопасность информационных технологий. 2016. № 3. С. 40–52.
9. Раскин А.В. Некоторые философские аспекты информационной войны // Информационные войны. № 3 (35) 2015. С. 18–21.
10. Розин В.М., Голубкова Л.Г. Управление в российском и мировом трендах. М., 2012.
11. 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.
12. Dibben M., Sheard S. Reason in Practice: A Unique Role for a ‘Philosophy of Management’ // Philosophy of Management. Sept. 2012. V. 11. Issue 3. Pp. 1–9.
13. Foerster H. Cybernetics of Cybernetics // Foerster H. Understanding Understanding. Essays on Cybernetics and Cognition. N.Y., 2003. P. 283–286.
14. Frolund L., Ziethen M. The Hermeneutics of Knowledge Creation in Organisations // Philosophy of Management. Sept. 2014. V. 13. Issue 3. Pp 33–49.
15. Gruzd A., Jacobson J., Wellman B., Mai P. Understanding Communities in an Age of Social Media: the Good, the Bad, and the Complicated // Information, Communication & Society. 2016. V. 19. Issue 9. Pp. 1187–1193.
16. Hooker C. Introduction to Philosophy of Complex Systems // Handbook of the Philosophy of Science. V. 10. Philosophy of Complex Systems. Oxford: Elsevier, 2012. Pp. 3–90.
17. McGregor I. Comparing Designers’ and Listeners’ Experiences // AI & Society. 2014. V. 29. Issue 4. Pp. 473–483.
18. Neira P. Values Regarding Results of the Information and Communication Technologies: Internal Values // New Perspectives on Technology, Values, and Ethics, Theoretical and Practical. (Boston Studies in the Philosophy and History of Science. V. 315). Dordrecht: Springer, 2015. Pp. 47–60.
19. Skeggs B., Yuill S. The Methodology of a Multi-model Project: Examining How Facebook Infrastructures Social Relations // Information, Communication & Society. 2016. V. 19. Issue 10. Pp. 1356–1372.

20. Emanuelson P., Willer D. External Threat as Coercion // Journal of Social Structure. 2015. V. 16, No 6. https://www.cmu.edu/joss/content/articles/volume16/EmanuelsonWiller.pdf (Available 15.10.2016).

REFERENCES:

1. Alekseev A. P., Alekseeva I. Ju. Informacionnaja vojna v informacionnom obshhestve // Voprosy filosofii. 2016. № 11. S. 5–14.
2. Arshinov V.I. Sinergetika vstrechaetsja so slozhnost'ju // Sinergeticheskaja paradigma. Sinergetika innovacionnoj slozhnosti. M., 2011. S. 47–65.
3. Golubkova L.G., Rozin V.M. Filosofija upravlenija. Joshkar-Ola: MarGTU, 2010.
4. Grachev G.V. Lichnost' i obshhestvo: informacionno-psihologicheskaja bezopasnost' i psihologicheskaja zashhita. M.: PER SJe, 2003.
5. Diev V. S. Racional'nye reshenija: kriterii, modeli, paradoksy // Voprosy filosofii. 2013. № 8. S. 4–11.
6. Diev V. S. Upravlenie. Filosofija. Obshhestvo // Voprosy filosofii. 2010. № 8. S. 35–41.
7. Maljuk A.A. Informacionnaja bezopasnost': konceptual'nye i metodologicheskie osnovy zashhity informacii. M.: Gorjachaja linija – Telekom, 2004.
8. Minaev V.A., Dvorjankin S.V. Obosnovanie i opisanie modeli dinamiki informacionno-psihologicheskih vozdejstvij destruktivnogo haraktera v social'nyh setjah // Bezopasnost' informacionnyh tehnologij. 2016. № 3. S. 40–52.
9. Raskin A.V. Nekotorye filosofskie aspekty informacionnoj vojny // Informacionnye vojny. № 3 (35) 2015. S. 18–21.
10. Rozin V.M., Golubkova L.G. Upravlenie v rossijskom i mirovom trendah. M., 2012.
11. Smoljan G.L., Zarakovskij G.M., Rozin V.M., Vojskunskij A.E. Informacionno-psihologicheskaja bezopasnost' (opredelenie i analiz predmetnoj oblasti). M.: In-t sistemnogo analiza RAN, 1997. 52 s.
12. Dibben M., Sheard S. Reason in Practice: A Unique Role for a ‘Philosophy of Management’ // Philosophy of Management. Sept. 2012. V. 11. Issue 3. Pp. 1–9.
13. Foerster H. Cybernetics of Cybernetics // Foerster H. Understanding Understanding. Essays on Cybernetics and Cognition. N.Y., 2003. P. 283–286.
14. Frolund L., Ziethen M. The Hermeneutics of Knowledge Creation in Organisations // Philosophy of Management. Sept. 2014. V. 13. Issue 3. Pp 33–49.
15. Gruzd A., Jacobson J., Wellman B., Mai P. Understanding Communities in an Age of Social Media: the Good, the Bad, and the Complicated // Information, Communication & Society. 2016. V. 19. Issue 9. Pp. 1187–1193.
16. Hooker C. Introduction to Philosophy of Complex Systems // Handbook of the Philosophy of Science. V. 10. Philosophy of Complex Systems. Oxford: Elsevier, 2012. Pp. 3–90.
17. McGregor I. Comparing Designers’ and Listeners’ Experiences // AI & Society. 2014. V. 29. Issue 4. Pp. 473–483.
18. Neira P. Values Regarding Results of the Information and Communication Technologies: Internal Values // New Perspectives on Technology, Values, and Ethics, Theoretical and Practical. (Boston Studies in the Philosophy and History of Science. V. 315). Dordrecht: Springer, 2015. Pp. 47–60.
19. Skeggs B., Yuill S. The Methodology of a Multi-model Project: Examining How Facebook Infrastructures Social Relations // Information, Communication & Society. 2016. V. 19. Issue 10. Pp. 1356-1372.
20. Emanuelson P., Willer D. External Threat as Coercion // Journal of Social Structure. 2015. V. 16, No 6. https://www.cmu.edu/joss/content/articles/volume16/EmanuelsonWiller.pdf (Available 15.10.2016).