УДК 331.103.226

М. С. Фабрикант

Белорусский государственный университет, *Минск*, *Беларусь*, *fabrykant@bsu.by*

ДОВЕРИЕ В ИНТЕРНЕТ-КОММУНИКАЦИИ КАК ФАКТОР ЭФФЕКТИВНОСТИ УПРАВЛЕНИЯ В ЭПОХУ ЦИФРОВИЗАЦИИ

В статье рассматривается роль доверия к информации и ее источникам в интернет-коммуникации в организационной среде. Указывается, что в отличие от макросоциального уровня, внутри организации оптимальным является не более высокое, не более низкое и не среднее, а дифференцированное доверие. Обосновывается неэффективность обучения сотрудников критической оценке сообщений, поступающих по интернет-каналам, посредством освоения ими процедур, выстроенных по принципу наивного байесовского классификатора, поскольку, помимо общей относительно небольшой эффективности такого рода алгоритмов, человеческое мышление, в отличие от искусственного интеллекта, плохо справляется с оперированием вероятностными закономерностями. Вместо этого предлагается обучение сотрудников следовать системе правил, основанной не на характеристиках интернет-сообщений, а на принципах работы с ними, встроенных в общую логику функционирования организации, что позволит обеспечить эффективность реализации управленческих решений.

Ключевые слова: *доверие, интернет-коммуникация, критическое мышление, управление, управленческие решения*

M. Fabrykant

Belarusian State University, *Minsk*, *Belarus*, *fabrykant@bsu.by*

TRUST IN INTERNET COMMUNICATIONS AS A FACTOR OF EFFICIENT MANAGEMENT IN THE AGE OF DIGITALIZATION

The article discusses the role of trust in information and its sources in Internet communication in the organizational environment. It is pointed out that, in contrast to the macrosocial level, within the organization the optimal solution is not a higher, lower or average, but differentiated trust. The article argues about the inefficiency of training employees to critically evaluate messages received via Internet channels by mastering procedures built on the principle of a naive Bayes classifier, since, in addition to the overall relatively low efficiency of this kind of algorithms, human thinking, unlike artificial intelligence, does not cope well with operating probabilistic rules. Instead, it is proposed to train employees to follow a system of rules based not on the characteristics of Internet messages, but on the principles of working with them, built into the overall logic of the organization's functioning, which will ensure the effectiveness of the implementation of management decisions.

Keywords: *trust, Internet communication, critical thinking, management, managerial decisions*

Социальное доверие стало в последние годы одной из популярнейших тем исследований в социальных науках. Отчасти это связано с тем, что рост социального доверия является одним из наиболее универсальных индикаторов неэкономической модернизации. Так, согласно теории модернизации ценностей Р. Инглхарта и К. Вельцеля [1], переход от материалистических ценностей к постматериалистическим, в частности, от ценностей самосохранения к ценностям самовыражения связан с тем, что люди начинают в большей степени доверять людям вообще, в т. ч. незнакомым людям. В то время как в традиционных обществах доверие ограничено только кругом близких и лично знакомых людей, как правило, связанных меду собой родственными узами, а в обществах раннего модерна договоренности с незнакомыми людьми, хотя в принципе возможны, требуют формальных, институционально закрепленных гарантий, то в обществах позднего модерна именно доверие является нормой, а представление о том,

что люди, в т. ч. лично между собой не знакомые, будут соблюдать договоренности даже в отсутствие эксплицитных формальных гарантий – опцией по умолчанию. Это неэкономическое измерение модернизации представляет особый интерес в силу своей связи с экономической модернизацией: на страновом уровне выявлена положительная корреляций между уровнем социального доверия в стране и ВВП на душу населения. Хотя за этой корреляцией могут скрываться различные каузальные механизмы, действующие в разных направлениях (например, можно предположить, что в странах с более высоким уровнем материального благосостояния у людей меньше стимулов нарушать договоренности), существуют серьезные основания полагать, что именно социальное доверие является одной из движущих сил роста ВВП на душу населения. Во-первых, в странах с более высоким уровнем доверия круг потенциальных деловых партнеров не ограничивается родственниками и давними личными знакомыми и людьми своего круга (т. е. теми, для кого нарушение договоренностей несет высокие репутационные издержки, превышающие потенциальную выгоду от нарушения договоренностей), но включает в себя всех, кто обладает нужными ресурсами, которые позволяют получить максимум выгоды от обмена. Во-вторых, априорное доверие к деловым партнерам существенно уменьшает объем необходимых трансакционных издержек, в данном случае прежде всего – издержек, направленных на обеспечение гарантий соблюдения договоренностей. Таким образом, высокий уровень социального доверия является если не одним из факторов, то, по крайней мере, важным индикатором модернизации и коррелятом экономического благополучия. Поэтому неудивительно, что социальное доверие до относительно недавнего времени воспринималось почти исключительно позитивно.

Отношение к феномену социального доверия стало меняться в связи с активизацией интереса к изучению того, как проявляется доверие во все более значимой сфере социальной жизни – в интернет-коммуникации. Изучение межличностного доверия дополнилось дифференцированным, отдельным от него изучением доверия к информации, а результаты эмпирических исследований разрушили первоначально односторонне оптимистичный взгляд на возможности, предоставляемые Интернетом. Исследования роли онлайн-образования в борьбе с социальным неравенством [2] показали, что для того, чтобы возможностями, которые предоставляет Интернет для доступа к высококачественной информации, одного наличия этих возможностей – предоставления информации и доступа к Интернету – недостаточно: нужен также определенный уровень мотивации, который проистекает из определенной трудовой этики, высокого уровня самоэффективности и наличия соответствующих ролевых моделей, с которыми человек может себя идентифицировать. При существующем неравномерном распределении этих факторов доступ к образовательным интернет-ресурсам может не только не уменьшать, но, напротив, закреплять и даже усиливать социальное неравенство. Прозрачность, которую Интернет как универсальное средство обмена информацией выводит на новый уровень, перестало восприниматься преимущественно как необходимое условие для понимания общества и его преобразования на более рациональных началах посредством коммуникативного действия и стало, напротив, рассматриваться как источник угроз частной жизни, что связано с проблемой кибербезопасности. Наконец, универсализация возможности создания и быстрого распространения информации привела к проблеме распространения фейковых новостей. Поэтому для того, чтобы сохранить выгоды от использования Интернета и при этом по возможности минимизировать связанные с ним риски, ключевым фактором оказалось формирование критического отношения к информации, т. е. низкого доверия, по крайней мере, низкого базового, безусловного доверия как опции по умолчанию.

Каким образом эту дилемму следует стремиться решить на уровне организации? Низкое доверие к информации, получаемой посредством интернет-коммуникации, как правило, приводит к тому, что внутрикорпоративные сообщения, получаемые по цифровым каналам, занимают в восприятии сотрудников неясную промежуточную позицию между устными сообщениями и содержанием нецифровых письменных документов. С одной стороны, как и устные сообщения,

многие формы интернет-коммуникации – сообщения в мессенджерах, по внутренней корпоративной сети и даже по корпоративной почте – могут быть необязательными для исполнения и лишенными какого-либо формального статуса. С другой стороны, в отличие от устных сообщений, цифровые формы коммуникации оставляют следы, причем удалить их полностью, т. е. без возможности восстановления существенно сложнее, чем бумажные документы. Эта двойственность порождает у сотрудников организации недоверие к использованию цифровых ресурсов для решения рабочих задач, особенно там, где формат такого использования внешне отличается от уже успевшей стать привычной неформальной интернет-коммуникации. Разумеется, это недоверие усугубляется в тех организациях, где для внешнего контроля за трудовой дисциплиной используется мониторинг за интернет-активностью сотрудников или ограничение доступа к определенным интернет-ресурсам, не связанным с работой. Помимо обширного блока проблем, связанных с подобными способами управления и более эффективными альтернативными возможностями повышения трудовой мотивации, рассмотрение которых выходит далеко за пределы данной работы, такие ограничения порождают общее недоверие к использованию средств интернет-коммуникации, поскольку избегать их оказывается более безопасно и менее когнитивно затратно, чем постоянное отслеживание того, какие ресурсы маркируются руководством как относящиеся к работе, а какие – расцениваются как неподходящие для использования в рабочее время. Этот достаточной крайний, хотя не столь редко встречающийся вариант демонстрирует ключевую управленческую задачу, связанную с интернет-коммуникацией. Эта задача заключается не в повышении и не в понижении доверия, в его большей дифференциации. Вопрос в том, каким образом эффективно обучить сотрудников различать получаемую посредством интернет-коммуникацию информацию и ее источники по степени достоверности и надежности.

Различные социально-психологические подходы к решению этой задачи сходятся в том, что простых и очевидных общих решений нет и быть не может. С точки зрения эволюционистского подхода, недостоверная (фейковые новости или внутриорганизационные сплетни, распространяющиеся по цифровым каналам) или опасная (фишинговые рассылки) информация, поступающая в организационную среду, начисто лишена внешних признаков, с которыми непроизвольно ассоциируется источник угрозы – такими, как громкие резкие звуки, необычно крупный размер, резкие быстрые движения. Поэтому автоматической реакции на такого рода угрозы ожидать не следует. С точки зрения социально-когнитивного подхода, оценка каждого сообщения, поступающего по интернет-каналам, как более или менее достойного доверия представляет собой сложную задачу, требующую существенных когнитивных усилий, поскольку необходимо постоянно держать в сознании достаточно большой список признаков недостоверной или опасной информации и оценивать по этим критериям каждое поступающее сообщение. По сути, такая процедура аналогична алгоритму наивного байесовского классификатора, который используется, например, для отфильтровывания спам-сообщений: первоначальная оценка вероятности того, что некое сообщение не заслуживает доверия затем корректируется в ту или иную стороны при обнаружении в нем тех отличительных черт, которые с большей или, напротив, меньшей вероятностью содержатся в ненадежных сообщениях, исходя из прошлого опыта. Помимо того, что алгоритмы такого рода сами по себе не слишком эффективны, такой способ информации человеческому мышлению дается значительно хуже, чем искусственному интеллекту, поскольку, как показали исследования основателей поведенческой экономики [3], оперировать вероятностными закономерностями – одна из самых трудных задач для человеческого мышления, наименее интуитивно понятная, как следствие, и наименее эффективно решаемая. В дополнение к этому, с точки зрения социально-конструктивистского подхода, проблема обучения сотрудников дифференцированному доверию в интернет-коммуникации – типичный случай того, как исследования, которые первоначально дают истинные результаты, приводят к видоизменениям собственного предмета, так что те же результаты перестают соответствовать действительности и в итоге

оказываются ложными. Дело в том, что обнаруживаемые типичные признаки недостоверных интернет-сообщений становятся известными не только тем, кто отвечает за организацию обучения кибербезопасному поведению и тем, кто это обучение проходит, но и тем, кто создает недостоверную информацию. Поэтому последние способны соответствующим образом модифицировать интернет-сообщения, чтобы избавить их от уже известных признаков, причем едва ли не быстрее, чем сотрудники организации обучатся их распознавать. Более того, ряд способов воздействия посредством распространения недостоверной информации, напротив, насыщается этими признаками, чтобы на стадии спам-рассылки отфильтровать наиболее доверчивых людей, на которых наиболее целесообразно затем оказывать адресное и существенно более затратное по времени воздействие.

Таким образом, можно сделать вывод, что обучение сотрудников дифференцированному доверию в интернет-коммуникации, основанное на характеристиках поступающих сообщений, относительно неэффективно, поскольку требует освоения сложных техник и постоянное переобучения. Поставленная задача требует иных управленческих решений. Одним из возможных решений, хотя, по всей видимости, далеко не единственным, может стать опора не на характеристики самих сообщений, а на правила, связанные с интернет-коммуникацией. Важно, чтобы эти правила не сводились к системе запретов и ограничений, но включали в себя представления не только о том, чего нельзя делать, что и о том, что делать можно и, главное, каким образом. Так, во внутрикорпоративной интернет-коммуникации необходимо определить, по каким каналам должны распространяться сообщения разной степени важности и разного статуса. Важно, чтобы сотрудники организации понимали логику такого распределения и характер доступа к разным внутрикорпоративным каналам для сотрудников с разными полномочиями и разными функциями в принятии управленческих решений. Что касается интернет-сообщений, поступающих извне, необходимо разработать единые протоколы, следуя которым, каждый сотрудник понимал бы, в каких случаях он может и обязан решить задачу самостоятельно, в каких – обратиться к своему непосредственному руководителю, а в каких – поставить в известность ответственных за кибербезопасность организации. Особое значение для этого имеет понимание того, в каких случаях стремление сотрудника перестраховаться или, напротив, проявить самостоятельность будет означать разумную предусмотрительность, а в каких – расцениваться как признак некомпетентность и грозить сотруднику «потерей лица». Для того, чтобы сотрудники при этом руководствовались не собственной индивидуальной склонностью к риску либо, напротив, риск-аверсивностью, а объективными характеристиками самой ситуации, необходимо разработать ясную и прозрачную систему правил, а в идеале – выстроить принятие решений, связанных с интернет-коммуникацией или, по крайней мере, в части кибербезопасности, как полноценный бизнес-процесс. Разумеется, при этом, несмотря на всю специфику предмета, закономерно могут проявиться не до конца или субоптимально решенные вопросы более общего плана, решение которых потребует более масштабных мер, к чему руководители, взявшиеся решать проблему доверия в интернет-коммуникации, должны быть готовы.

Список использованных источников

1. *Инглхарт*, *Р.* Культурная эволюция. Как изменяются человеческие мотивации и как это меняет мир / Р. Инглхарт – М : Мысль, 2018. – 347 с.

2. *Hansen*, *J. D.* Democratizing education? Examining access and usage patterns in massive open online courses / J. D. Hansen, J. Reich // Science. – 2015. – V. 350. – № 6265. – P. 1245–1248.

3. *Tversky*, *A.* Availability: A heuristic for judging frequency and probability / A. Tversky, D. Kahneman // Cognitive psychology. – 1973. – V. 5. – №. 2. – P. 207–232.