СОЦИАЛЬНО-ТЕХНОЛОГИЧЕСКИЕ ПРОБЛЕМЫ И ИНФОРМАТИЗАЦИЯ ПРЕДПРИЯТИЙ И ОРГАНИЗАЦИЙ

Зернов С.В.

Институт проблем управления им. В.А. Трапезникова,
Россия, г. Москва, ул. Профсоюзная, д.65
5219528@mail.ru

Аннотация: Рассмотрены проблемы внедрения ИТ систем на предприятиях и организациях, риски и угрозы информационной безопасности в связи с использованием ИИ, положительные и отрицательные стороны информатизации для общества. Показана особая роль самоорганизующихся команд как перспективной социальной технологии для решения задач социального развития.

Ключевые слова: социальные технологии, информационные технологии, искусственный интеллект, самоорганизующиеся команды, социальная деградация.

Введение

В начале развития авиации было очевидно, что скорости самолетов будут только расти. Сегодня люди летают на самолетах с теми же скоростями, что и пятьдесят лет назад. Большинство из них тратят на предполетную подготовку времени в разы больше, чем на сам перелет из-за проблем с транспортной безопасностью. Судя по темпам нарастания мошенничества в банковской сфере нас ждет та же ситуация и в сфере информатизации. Недалеко то время, когда общество с тоской станет вспоминать, как легко и быстро можно было выполнить операцию через грамотного операциониста банка сравнивая с тем, какие временные затраты, проблемы и риски несет за собой даже простая операция оплаты билетов на самолет или отеля через Интернет. Возможность обратиться к операционисту, конечно, останется. Однако такая роскошь будет доступна только привилегированным клиентам, которые и сегодня могут позволить летать на бизнес-джетах. За счет всех тех, кто построил и обслуживает самолеты, аэропорты и страну в целом.

Хотя большинство людей еще об этом даже не задумались, но множество фактов говорит о том, что привычная всем компьютеризация практически исчерпала свои возможности. Перестал выполняться закон Мура. Рост производительности компьютеров уже давно не приводит к пропорциональному повышению эффективности их использования. Распараллеливание вычислений упирается в пределы обусловленные законом Амдала. Создание многопоточных систем приводит к появлению новых типов ошибок из-за проблем взаимной блокировки, нарушений последовательности выполнения параллельных операций и т.п. Эпоха информатизации, посредством автоматизации существующих бизнес-процессов на предприятиях и в организациях, тоже подходит к своему логическому завершению. Сложившиеся в прошлом подходы к информатизации теперь создают больше проблем, чем решают, при экспоненциальном росте затрат на информатизацию. Аналогичные проблемы возникают при стремлении, например, обвешать камерами скорости каждый метр дороги, приводя к астрономическим затратам бюджета, многомиллиардным долгам по необоснованным штрафам никак не влияющим на безопасность дорожного движения. Но уже многим вполне понятно, что не ради безопасности дорожного движения они размещаются, а ради пополнения бюджета из которого можно беспрепятственно и бесконтрольно растрачивать и разворовывать народные деньги.

С момента внедрения информационных систем быстро стало очевидно, что информатизация хаоса не только не улучшает, но еще больше снижает эффективность выполнения производственных и управленческих функций, цементируя неэффективные социально-технологические процессы. Как на промышленных предприятиях и частных фирмах, так и в бюджетных учреждениях и общественных организациях. Временным решением стало использование моделирования бизнес-процессов, методологически опиравшееся на принципы разработанные в исследовании операций, адаптированные для задач бизнеса. Однако, если автоматизация технологических производственных операций была очевидным прогрессом, то для общественных организаций такой подход к информатизации оказался абсолютно непригоден. В итоге все усилия теперь сконцентрированы вокруг облегчения и расширения способов осуществления социальных коммуникаций. Которые, к сожалению, все чаще используются для манипулирования в социальных сетях и оболванивания людей. Ожидаемого прорыва от появления распределенных баз знаний и интеллектуальных систем управления не наблюдается. Наоборот, происходит стремительная деградация общества во всех областях — морального и нравственного, умственного и физического.

1 Социально-технологические проблемы внедрения ИТ систем

Буквально каждое современное предприятие или организация имеет множество собственных информационных систем и поставляет информацию во внешние информационные системы. Для этого им потребовалось осуществить автоматизацию бухгалтерии и систем документооборота, создать систему для взаимодействия с клиентами и аналитическую систему для целей управления и т.д. Все это создает представление о неограниченных возможностях и грандиозных будущих перспектив для общества от применения информатизации для управления предприятием и организацией. Однако так ли хорошо обстоят дела на самом деле? У многих топ менеджеров и руководителей среднего звена создалось впечатление, что внедрение ИТ систем не представляет собой особых трудностей. И если для автоматизации ритейла это соответствует действительности, то для предприятий и остальных организаций все оказалось не так просто. Эффект экономии на издержках и магия упорядоченности бизнес-процессов создали ложное ощущение, что информатизация позволяет запросто решить любые проблемы управления. Однако в реальности, как показывает практика, эти проблемы не просто никуда не делись, а усугубились. Что наглядно проявляется в ходе исследовании проблем управления проектами в российской ИТ сфере [1]. Из них можно сформировать следующие пять групп:

Корпоративная бюрократия и передел сфер влияния внутри компании

- Использование ИТ проектов как средства получения преимущества перед другими менеджерами высшего звена: ради карьерного роста или личной выгоды, перераспределения прибыли внутри организации и даже мести другим сотрудникам
- Корпоративные бюрократические процедуры препятствующие развитию предприятия: незыблемые формальные правила и тщательно скрываемые неформальные подходы, негласные договоренности и групповые интересы
- Необоснованные ожидания и неопытность руководства в части реализации ИТ проекта: неоправданно короткие сроки реализации проекта или низкая численность исполнителей проекта на предприятии, недостаточный бюджет или недофинансирование проекта

Проблемы неподготовленности кадров

- Низкий уровень квалификации исполнителей
- Сопротивление изменениям со стороны сотрудников предприятия
- Одновременное использование одних и тех же исполнителей в нескольких проектах

Проблемы качества корпоративного управления

- Отсутствие необходимой поддержки и своевременного участия со стороны высшего руководства, приводящее к серьезным препятствиям и переносам сроков реализации ИТ проекта
- Неоправданное расширение результатов применения ИТ в отдельном подразделении на все предприятие или организацию, в результате чего может обнаружиться неприемлемость такого подхода
- одновременное выполнение нескольких ИТ проектов, приводящее к перегрузке сотрудников и несогласованности при внедрении нескольких ИТ проектов

Проблемы компетенции менеджмента в области внедрения ИТ

- Необоснованное использование эталонных моделей, концепций и стандартов в области управления ИТ существенно снижающие как возможность успешной реализации проекта, так и удовлетворенность его результатами
- Низкий уровень зрелости ИТ инфраструктуры приводящий к ограниченности функционала из-за неготовности существующих компонентов для функционирования вместе с внедряемой ИТ системой
- Сложности интеграции внедряемой ИТ системы с используемыми на предприятии ИТ продуктами, влекущие за собой резкий рост затрат на внедрение и срыв сроков из-за высоких издержек и неожиданных препятствий

Организационные проблемы

- Низкий уровень зрелости бизнес-процессов предприятия, отсутствие регламентов и распределения функциональных обязанностей сотрудников предприятия
- Сложность получения необходимой информации при определении функциональных требований к ИТ проекту и при его реализации;
- Постоянная корректировка приоритетов, требований и содержания ИТ проекта;

Увлечение информатизацией отчасти подменило, а иногда и просто стало препятствием для развития современных организаций. Информатизация позволила выявить неэффективные производственные процессы и резко повысить производительность обработки служебной информации, что способствовало повышению рентабельности деятельности. Это способствовало получению дополнительной прибыли и создало возможность отложить решение задач стратегического развития. Однако предприятия и организации, на которых основные бизнес-процесс автоматизированы, уже не могут повысить свою рентабельность и результативность за счет информатизации данных операций. А автоматизировать нестандартные или временные операции нет смысла, так как это дороже, чем обрабатывать их вручную.

Процедуры стратегического планирования и, тем более, поиска новый путей развития бизнеса, требуют развитых навыков корпоративного планирования и большого управленческого опыта. В условиях тотальной конкуренции от этих решений напрямую зависит уже не столько рентабельность коммерческих предприятий и эффективность деятельности организаций, сколько их выживание в принципе. Для примера можно вновь вспомнить авиаперевозки. Автоматизация пилотирования самолетов привела к проблемам при нештатных операциях. Около 80% гибели воздушных судов приходится на ошибочные действия пилотов.

Наконец, информатизация и роботизация приводит к высвобождению большого количества работников. Применение систем автоматизации для замены человека приведет к потере целых отраслей бизнеса. Например, как это произошло с операциями по перемещению груза на закрытых территориях в портах, и, в ближайшем будущем, ожидается в автомобильных перевозках на дорогах общего назначения. Что создает уже перед государствами новые неожиданные экономические проблемы и ведет к перманентной социальной нестабильности. А желающих этим воспользоваться в современном мире найдется немало...

2 Социально-технологические проблемы безопасности ИТ систем

Согласно результатам исследований [2] производителя антивирусов McAfee и Центра стратегических и международных исследований (CSIS) ущерб мировой экономики от хакерских атак в 2020 году составил триллион долларов. Это на 50 процентов больше, чем два года назад. В этом же году МВД России сообщало, что более половины от всех совершенных мошенничеств составляют преступления с использованием информационно-телекоммуникационных технологий [3].

Компания Trend Micro, совместно с Межрегиональным научно-исследовательским институтом ООН по вопросам преступности и правосудия и Европолом подготовили обзорный доклад по результатам изучения возможных опасностей от использования злоумышленниками искусственного интеллекта [4]. В нем исследуется, как мошенники используют ИИ сейчас, какие способы могут распространиться в будущем. На основе их исследования можно выделить существующие и перспективные возможности применения ИИ для ссовершения мошеннических действий и киберпреступлений.

Использование ИИ для повышения эффективности действий злоумышленников

- вполне очевидно, что ИИ будет применяться злоумышленниками для повышения эффективности вредоносного ПО и фишинга. Как используя традиционные методы проникновения на компьютеры пользователей через Интернет и системы хранения данных, так и проникая в облачные хранилища
- использование ИИ обеспечивает возможность быстрого и эффективного подбора паролей. Что станет проблемой для огромного количества пользователей имеющих доступ к многочисленным системам посредством простых паролей. Сделанные ранее различные опросы и исследования неоднократно подтвердили, что люди используют несложные пароли, которые можно легко вспомнить. Применение систем ИИ для подбора паролей потребует от пользователей перехода на электронные ключи, которые не должны храниться на самих устройствах, так как оттуда тоже могут быть украдены
- ИИ уже сейчас применяются для целей шифрования и даже позволяют создавать секретные ключи без участия человека [5]. Разрабатываются различные системы с использованием ИИ для улучшения качества шифрования. Коммерческие реализации таких разработок или альтернативные разработки на их основе могут использоваться для создания систем для взлома электронных шифров или их перехвата
- системы распознавания лиц и изображений с использованием ИИ. Применение ИИ позволит создавать поддельные изображения и видео записи на основе реальных изображений. С их помощью можно будет осуществлять подделку документов, создавать компрометирующие

материалы на граждан и общественных деятелей, распространять дезинформацию в Интернете и осуществлять манипулирование в социальных сетях

- применение ИИ для обработки больших информационных массивов для получения данных банковских карт и номеров телефонов. Применение систем ИИ позволит извлекать такие данные не только из обычного текста, но и в результате обработки изображений и видео. Через доступ к корпоративным серверам с помощью социальной инженерии злоумышленники получат возможность обработки средствами ИИ корпоративных баз данных с целью извлечения из них персональных данных сотрудников, номеров их банковских карт и размеров доходов. Организованные преступные группировки и конкуренты смогут использовать ИИ для сбора информации из корпоративных систем о финансовых операциях, оффшорных счетах предприятий и связях с коррумпированной бюрократией.

Перспективы использования ИИ злоумышленниками в ближайшем будущем

- уже существуют генераторы текста, которые могут создавать текст который трудно отличить от текста написанного человеком. Генерация текстов с фиксированным словарным запасом и имитация стилистики конкретного человека позволит создавать персонализированные тексты и направлять электронные сообщения сотрудникам компании с указанием на выполнение финансовых переводов на подставные счета. Подобный успешный опыт уже имеется даже с генерацией голоса посредством ИИ обеспечивший денежный перевод в рамках корпоративных процедур [6]
- большое распространение ИИ может получить для мошеннических действий посредством социальной инженерии. Они могут использоваться с целью обмана систем идентификации, использующие биометрические данные или предназначенные для распознавания автоматизированных действий. Данные полученные из медицинских систем позволят применять методы социальной инженерии для воздействия на уязвимые места людей с различными заболеваниями и их шантажа, применения лекарственных средств с целью ухудшить их состояния здоровья и воздействовать на психику и т.д.
- широкие возможности открываются при использовании ИИ для имитации человеческого поведения в социальных сетях. Генерация активности похожей на действия реального человека посредством лайков, посещения интернет-сайтов, прослушивания музыки, создания комментариев к постам и т.п. Такое поведение может сделать бессмысленным защитные системы созданные для выявление ботов.
- ИИ прекрасно подходит для генерации подобия человеческого голоса и использования его для получения доступа к сервисам банков активируемых голосовыми сообщениями и действий с фондовыми и валютными активами посредством приказов через брокерские компании
- использование ИИ для масштабных финансовых операций. Прежде всего, на нерегулируемых рынках различных крипотовалют с целью осуществления незаконной торговли криптовалютами в интересах преступных кланов и корпоративных мошенников. С использованием ИИ могут быть взломаны системы алгоритмического трейдинга или маскироваться торговля на фондовых рынках на основе инсайдерской информации
- - подключение все большего числа гаджетов и распространение Интернета вещей позволит злоумышленникам использовать ИИ для создания различных сценариев управления бытовой техникой и получения несанкционированного доступа в помещения, сбора личных данных и незаконного сбора сведений о личной жизни
- серьезную общественную опасность представляет использование ИИ для осуществления террористических действий или вымогательства посредством вмешательства в работу и движение общественного транспорта, управления движением поездов и воздушных судов, управления гидро- и атомными электростанциями. В отношении последних уже зафиксировано достаточное число случаев с внедрением в данные системы вирусов с целью перехвата управления ими [7]
- широкое использование беспилотных летательных аппаратов и автомобилей может позволить применить ИИ для подмены изображений и захвата управления ими или предоставления этим системам ложных данных от других транспортных средств с которыми создана локальная группа при их совместном движении. Что может использоваться для создания аварий в нужное время и причинении вреда имуществу и людям, вплоть до их использования в качестве орудий для умышленных убийств
- применение ИИ спецслужбами для целей разведки и военными для управления запуском или перенаправления движения запущенных ракет. Кому то это может показаться выдумкой, если

бы не тот факт, что еще в 1971 году между США и СССР было подписано соглашение о действиях в случае несанкционированного запуска ядерных ракет [8]. В то время еще никто представить себе не мог какое будет создано количество компьютерных систем и масштабы распространения Интернета, хотя он уже и был создан. Теперь, когда мы вроде бы и осознаем, что технологии используются разными людьми и для решения тех задач, которые они перед собой ставят. Но понятия не имеем, что с этим делать

- в отдаленной перспективе ИИ позволят обманывать различные системы основанные или использующие системы ИИ. Так как сами системы ИИ не позволяют человеку полностью проверить действия на основе которых осуществляется выбор, что позволит вмешиваться и искажать работу самих систем ИИ.

Все перечисленное создает впечатляющее представление о том, каким угрозам уже подвергается и неизбежно будут подвергаться информационные системы. Однако трудно себе представить какую опасность и для какого количества людей может представлять комбинация нескольких этих угроз и насколько легко она может быть осуществлена. Тем более, когда сообщения о событиях в борьбе за рынки сбыта постоянно занимают центральные полосы газет и популярных новостных интернет-порталов, а борьба с киберпреступностью чуть ли не последнее. И все это меркнет перед возможностями корпораций, которые легально за счет самих людей и с использованием их талантов создают компьютерные системы и информационные среды с целью манипулирования этими же людьми, ради максимизации прибыли. Возможности ИИ оказываются ничтожными по сравнению с деятельностью естественного интеллекта социальных паразитов, которые смогли так организовать механизм глобальной социальной конкуренции, что места ничему человеческому на Земле в перспективе уже и не просматривается.

3 Социально-технологические проблемы обусловленные применением ИТ систем

Вроде бы давно уже очевидно, что технологии лишь обслуживают человеческие устремления и могут позволить решать задачи более эффективно и оперативно. А, значит, сами по себе не могут сделать человека лучше или хуже. Однако они могут ускорить эти процессы настолько, что человек просто не успеет справиться с тем, что с ним произойдет. В этом смысле компьютер тоже является инструментом, который усиливает возможности и ускоряет социальные процессы. Как положительные, так и отрицательные. В работе [9] представлена таблица 1 К.Хессинга в которой отражены положительные и отрицательные последствия компьютеризации.

Таблица 1. Положительные и отрицательные последствия компьютеризации

Положительные последствия	**Отрицательные последствия**
КУЛЬТУРА И ОБЩЕСТВО	
Свободное развитие индивида	"Автоматизация" человека
Информационное общество	Дегуманизация жизни
Социализация информации	Технократическое мышление
Коммуникативное общество	Снижение культурного уровня
Преодоление кризиса цивилизации	Лавина информации
	Элитарное знание (поляризация)
	Изоляция индивида
ПОЛИТИКА	
Расширение свобод	Снижение свобод
Децентрализация	Централизация
Выравнивание иерархии власти	Государство-"надзиратель"
Расширенное участие в общественной жизни	Расширение государственной бюрократии
	Усиление власти благодаря знаниям
	Усиление манипуляции с людьми
ХОЗЯЙСТВО И ТРУД	

Положительные последствия	Отрицательные последствия
Повышение продуктивности Рационализация	Все возрастающая сложность жизни
Повышение компетенции Увеличение богатства	Обострение промышленного кризиса
Преодоление кризиса	Концентрация
Экономия ресурсов	Подверженность кризисам
Охрана окружающей среды	Стандартизация
Децентрализация промышленности Новая продукция	Массовая безработица Новые требования к мобильности трудящихся
Улучшение качества	Дегуманизация труда
Диверсификация продукции	Стрессы
Новые профессии и квалификации	Деквалификация. Исчезновение многочисленных профессий.
МЕЖДУНАРОДНЫЕ ОТНОШЕНИЯ	
Национальная независимость	Усиление взаимозависимости
Появляется шанс на развитие у стран "третьего мира"	Технологическая зависимость. Обострение отношений Юга-Запада
Улучшение обороноспособности страны	Уязвимость. Усиление опасности новой войны из-за обновления военных систем

4 Возрастающая роль самоорганизующихся команд

Социальная изменения и бурный рост промышленного производства привели к изменению в условиях существования и жизни не только отдельного человека, но и человечества в целом. Создание огромных городов (социальная скученность, опасные соседства, сложная и уязвимая инфраструктура и т.п.) и изменения ландшафта (засорение пластиками, хищническая вырубка лесов, исчерпание полезных ископаемых и т.п.) приводит к экономическим и экологическим проблемам быстрее, чем люди осознают и понимают, как эти задачи решать. Традиционные иерархические организации, тем более бюрократические государственные структуры не успевают за происходящими в обществе изменениями. Неспособность оперативно изменять свое функционирование приводит к катастрофическим запаздываниям, создавая проблемы как для работы предприятий и организаций, так и для жизни общества.

Естественно, в таких условиях, гибкие методы проектирования и организации деятельности начинают теснить традиционные методы. Не только в части управления отдельными проектами, но и даже управления целыми организациями. Данная тенденция отчетливо видна в востребованной обществом отрасли ИТ, где производство программного кода поставлено на поток для его исполнения на устройствах с кремниевым арифмометром. Столкнувшись с неповоротливостью иерархических организаций разработчики программного обеспечения стремятся избавиться от нечетких постановок задач и неспособности заказчиков формулировать свои ожидания. Для этого они вынуждены искать новые способы организации своей командной работы. Поэтому нет ничего удивительного, что в ИТ сфере растет интерес к самоорганизации командной работы.

Чтобы лучше понять суть команды следует рассмотреть ее в условиях близких к антагонистическому социальному конфликту – активному противоборству и, даже, войне. Под военной командой традиционно понимается небольшой отряд войск, посылаемый для исполнения конкретного задания. Отряд действует автономно с целью выполнения боевой задачи, поставленной вышестоящим командованием. В связи с чем перед командиром возникает необходимостью координации совместных действий всех участников команды. Такая координация приводит к необходимости коллективного обсуждения плана действий и согласования порядка их исполнения тем интенсивнее, чем сложнее боевая задача. Поэтому в военных условиях самоорганизация команды оказывается естественной реакцией на необходимость выжить и выполнить задание. Собственно возможность самостоятельно решать локальные боевые задачи принципиально отличает команду от регулярных войск. И, по-сути, такая команда оказывается аналогом штабного командования. С той лишь разницей, что ошибки разведывательной команды могут привести к ее частичной или полной

гибели, а за ошибочные решения командования своими жизнями расплачиваются рядовые солдаты и младшие офицеры. Жизнь же самих генералов, пока они не попали в окружение или война не проиграна, не подвергается непосредственной опасности. Таким образом, навыки командной работы формируются в самых малых мобильных боевых отрядах и в штабах на каждом уровне военной иерархии. Именно эти две группы приобретают навыки командной работы. В то время как вся остальная подавляющая часть войска навыков самоорганизации не приобретает.

Примерно аналогичные процессы протекают на предприятиях и в организациях. Хотя интенсивность обсуждений меньше, да и социальная опасность в них существенно ниже. Самая печальная ситуация имеет место в процессах самоорганизации гражданского общества. Единственной причиной его консолидации и планирования совместных действий до сих пор остается общая внешняя смертельно опасная угроза. Чего явно недостаточно для перехода от самоуправства властей к народному самоуправлению [10].

5 Самоорганизующиеся команды и внешнее управление

В привычном смысле под командой в бизнесе понимается группа людей, призванная выполнить определенную работу под руководством лидера. В последние двадцать лет в развитых странах особую роль в развитии бизнеса стали играть самоорганизующиеся команды. Самоорганизующаяся команда – это команда, которая берет на себя ответственность за выработку и исполнение своих решений. В лучшем случае совместная работа такой команды окажется наилучшим средством достижения поставленных целей. Для этого в самоорганизующейся команде должен быть налажен механизм обратной связи, умение строить цели и гипотезы для осуществления их проверки, развивать навыки эффективного взаимодействия. Успешная самоорганизация обеспечивает поддержку членов команды, поддержку со стороны менеджмента и ценность для всей организации в целом. Лидер команды занимается развитием людей, позволяя команде самостоятельно решать возникающие проблемы, помогает улучшать отношения и способствует положительным переменам.

Для сформировавшейся команды характерно стремление к достижению общей цели, солидарной ответственности за выполнение общих планов, доверие и открытое обсуждение новых идей.

Помимо лидера особую роль в жизни команды играет внешний руководитель. Согласно результатам исследования [11] эффективное управление самоорганизующихся команд внешними руководителями требует особого подхода и может быть описано четырьмя базовыми функциями: установление контактов, разведка, убеждение и наделение полномочиями.

Установление контактов

Внешние руководители должны постоянно общаться со своей командой и остальной компанией, чтобы выстроить систему взаимоотношений. Успех здесь зависит от действий по трем направлениям: социальной и политической осведомленности, построения доверия в команде и заботы о членах команды.

1. Социальная и политическая осведомленность. Грамотный внешний руководитель демонстрируют понимание внутриорганизационной атмосферы, писанных и неписанных правил.

2. Построение доверия в команде. Лучшие внешние руководители понимают важность построения хороших отношений со своими командами, вплоть до приобретения статуса «своего».

3. Забота о членах команды. Средние внешние руководители зачастую воспринимают личные проблемы членов команды как помехи к достижению цели, в то время как лучшие внешние руководители чаще видят в них возможности для установления отношений с людьми.

Разведка

Для проведения эффективной «разведки» внешний руководитель должен действовать в трех направлениях: искать информацию; диагностировать поведение членов группы; систематически анализировать проблемы.

4. Поиск информации. Информацию можно использовать для влияния на принятие решений в команде. Руководитель, получающий развернутую информацию, гораздо эффективнее отстаивает интересы своей команды. А те, в свою очередь, сами приходят к пониманию значимости фигуры внешнего руководителя.

5. Диагностика поведения членов группы. Из-за того, что внешний руководитель обычно отвечает за работу нескольких самоорганизующихся команд, он редко присутствует когда в какой-то группе происходит нечто критичное. Восполнять недостаток информации приходится задним числом и также постфактум пытаться исправить то, что зачастую исправить уже нельзя.

6. Систематический анализ проблем. При первых признаках проблем лучшим руководителям свойственно систематически и скрупулезно вникать в ситуацию. Собирая информацию из первых

рук, у членов группы, руководитель может точно оценить ее перспективы, что позволяет ему давать аргументированные рекомендации как для своей группы, так и для других внешних групп влияния.

Убеждение:

Эффективное убеждение в условиях внешнего руководства требует активности в двух направлениях: внешней поддержки и влияния на команду.

7. Внешняя поддержка. Часто команды нуждаются в помощи организации и обеспечение этой поддержки – задача внешнего руководителя.

8. Влияние на команду. Эффективные внешние руководители отлично умеют склонить свою команду к принятию тех решений, которые лучше всего отвечают потребностям организации. Ключевыми условиями для этого являются доверие команды и информация из внешних источников.

Наделение полномочиями

Наделение полномочиями осуществляется по следующим трем направлениям: передача полномочий, гибкий подход к командным решениям и тренинг.

9. Передача полномочий. Внешние руководители располагают значительной свободой в принятии решений о том, какие именно полномочия и в каком объеме они передают командам. При этом лучшие внешние руководители стремятся передать своим командам больше ответственности.

10. Гибкий подход к командным решениям. Команды могут предлагать решения, которые не подходят для организации или не являются правильными. В таком случае средние внешние руководители выступают против, а лучшие руководители проявляют уважение к чужому мнению.

11. Тренинг. Тренинг подразумевает несколько разных видов деятельности, включая индивидуальную работу с сотрудниками, обеспечение обратной связи с командой и демонстрацию определенных приемов и поведения. Лучшие внешние руководители активно обучают свои команды. Внешние руководители должны постоянно развивать свои команды, чтобы те становились все более независимыми.

Заключение

Привычные подходы к информатизации, тем более механистическая цифровизация, не могут избавить общество от того нарастающего шквала социальных проблем, который возникает в связи с ее использованием. Так как в настоящее время информатизация используется преимущественно для автоматизации алгоритмических процедур или фиксирования перестроенных бизнес-процессов. При этом новые подходы, учитывающие особенности человеческого взаимодействия, не могут быть построены на их основе. Требуется принципиально иной взгляд на проектирование информационных систем коммерческих предприятий и общественных организаций, основанный на знании особенностей социальных взаимодействий и способствующий разрешению, а не усугублению социальных проблем. Поэтому, в свою очередь, он должен опираться на фундаментальные закономерности и изученные представления о социальных взаимодействиях. Однако, к сожалению, базовые основы социальных взаимодействий изучены еще недостаточно, в отличие от прикладных знаний и навыков, применяемых с целью манипулирования конкретными людьми и паразитировании на обществе в целом.. В результате самой развивающейся сферой стал социальный инжиниринг и хакерство, активно и успешно использующие безграмотность народных масс в области информационной безопасности и многочисленные уязвимости систем информационной безопасности предприятий и организаций.

Выходом из грядущего застоя или даже приближающегося тупика может стать создание адаптивных информационных систем, способных быстро приспосабливаться под изменения в социально-технологических процессах. При которых учитывается потребность субъекта, участвующего в социальном взаимодействии, в решении не только задач стоящих перед предприятием или организацией, но и достижения собственных стратегических планов своей жизни. Которые, все чаще, оказываются для него приоритетнее, чем коммерческие интересы корпораций.

Создателями таких систем могут стать самоорганизующиеся трудовые коллективы и производственные команды, включающие в себя заинтересованные стороны. Начиная с представителей производителя услуги, включая консультантов по управлению и специалистов по информатизации, заканчивая конечным потребителем услуги. Сам процесс совместной деятельности может быть реализован в виде встречного проектирования посредством мозговых штурмов. В совокупности именно результат их совместной проектной деятельности и будет приводить к изменению социальной действительности и влиять на будущее предприятий и организаций.

Наивно было бы полагать, что самоорганизующиеся команды станут панацеей для избавления от всех бед. Просто потому, что самоорганизующиеся команды - это тоже технологии. Пусть

социальные, а не информационные. Но, по-прежнему, технологии. Хотя в этом, безусловно, существует огромная разница. Так как социальные технологии, все-таки, оказываются существенно ближе к человеку, чем процедуры программирования кремниевых арифмометров. Под прикрытием необходимости технологического развития которых активно насаждаются огромным массам людей совершенно дикие и античеловеческие идеи, организуется их тотальная деградация и т.п. Поэтому главный вопрос, который необходимо решать - это превращение самоорганизующихся команд в самоуправляемые дееспособные коллективы. Которые способны сами определять свои цели и выбирать допустимые их способы достижения. Для которых важнейшей задачей станет способность научиться избавляться от своих ошибочных взглядов и навязанных ложных представлений - Химер. И осуществлять самообучение навыкам критического мышления, чтобы уметь дифференцировать реальную созидательную деятельность от опасных порывов и патологических устремлений. Как в себе самих, так и среди множества тех людей, которые наивно полагают свои действия созидательными или тщательно скрывают свои паразитическую сущность. Без таких команд гражданское общество не только не сможет оказать существенное влияние на дальнейшее развитие общества, но в недалеком будущем само по себе перестанет существовать как социальное явление.

Литература

1. *Курочкин Д.Э.* Современные проблемы управления инновационными проектами информатизации предприятия // Современные проблемы науки и образования. – 2014. – № 6.
2. *Елена Гункель* Ущерб от хакерских атак в мире превысил триллион долларов //Русская редакция Deutsche Welle - 07.12.2020 https://p.dw.com/p/3mNHm Дата обращения 01.06.2021
3. В МВД назвали долю мошенничеств, которые совершаются с помощью IT https://tass.ru/obschestvo/8283043Дата обращения 01.06.2021
4. Malicious Uses and Abuses of Artificial Intelligence https://documents.trendmicro.com/assets/white_papers/wp-malicious-uses-and-abuses-of-artificial-intelligence.pdf Дата обращения 01.06.2021
5. *Martín Abadi, David G. Andersen* Learning to Protect Communications with Adversarial Neural Cryptography //arXiv:1610.06918v1 21 Oct 2016 https://arxiv.org/abs/1610.06918 Дата обращения 01.06.2021
6. *Catherine Stupp* Fraudsters Used AI to Mimic CEO’s Voice in Unusual Cybercrime Case Aug. 30, 2019 https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402 Дата обращения 01.06.2021
7. *Дмитрий Конухов* Вакцина для атома: кибербезопасность АЭС 16 ноября 2015 https://russiancouncil.ru/analytics-and-comments/analytics/vaktsina-dlya-atoma-kiberbezopasnost-aes/ Дата обращения 01.06.2021
8. *Sherman Frankel* Aborting Unauthorized Launches of Nuclear-armed Ballistic Missiles through Postlaunch Destruction //Science & Global Security, 1990, Volwne 2, pp.1-20 or http://scienceandglobalsecurity.org/archive/sgs02frankel.pdf
9. *Ракитов А. И.* Философия компьютерной революции.— М.: Политиздат, 1991.—287 с.
10. *Зернов С.В.* Системные проблемы государственного управления как угроза национальной безопасности / Материалы 28-й Международной конференции «Проблемы управления безопасностью сложных систем» (ПУБСС'2020, Москва). М.: ИПУ РАН, 2020. С. 53-56.
11. *Vanessa Urch Druskat and Jane V.* How to Lead a Self-Managing Team 2 July 15 2004 https://sloanreview.mit.edu/article/how-to-lead-a-selfmanaging-team/ Дата обращения 01.06.2021