МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ВСЕРОССИЙСКИЙ ИНСТИТУТ НАУЧНОЙ И ТЕХНИЧЕСКОЙ ИНФОРМАЦИИ
РОССИЙСКОЙ АКАДЕМИИ НАУК
(ВИНИТИ РАН)

НАУЧНО • ТЕХНИЧЕСКАЯ ИНФОРМАЦИЯ

Серия 1. ОРГАНИЗАЦИЯ И МЕТОДИКА ИНФОРМАЦИОННОЙ РАБОТЫ

ЕЖЕМЕСЯЧНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ СБОРНИК

Издается с 1961 г. **№ 3** **Москва 2022**

ОБЩИЙ РАЗДЕЛ

УДК 004.056:002:316.4

О.В. Сюнтюренко

Прогнозирование потенциальных угроз и мегарисков развития информационных технологий*

В наш век стремительного развития технологий любая
локальная проблема может стать мировой

Рассматриваются методологические аспекты прогнозирования возникновения угроз и рисков развития информационных технологий на основе многокритериального анализа взаимодействия человека с информационной средой, а также проблемы информационной безопасности личности и социума с учетом влияния таких факторов, как глобализация мировой экономики и формирование нового технологического уклада. Информатизация, конвергенция компьютерных, телекоммуникационных технологий и мультимедиа обеспечивают принципиально новый уровень цивилизационного развития, все более влияя на жизнь человека и общества. С позиций системного подхода, применения методов наукометрии и многомерного анализа ис-

* Статья подготовлена в рамках работ по гранту РФФИ № 20-07-00014 «Разработка методологии использования наукометрических данных для решения задач целеполагания, прогнозирования и управления научными исследованиями».

следуются причинно-следственные связи возникновения наиболее опасных и значимых угроз и рисков внедрения информационных технологий для экономики и общества в целом. Сформулированы некоторые выводы, первоочередные и наиболее актуальные задачи разработки междисциплинарной проблемы прогнозирования оценки и минимизации рисков развития информационных технологий.

Ключевые слова: *информационные технологии, риски, социальные сети, информационная безопасность, манипуляции сознанием, цифровое неравенство, трансформация личности, цифровая зависимость, конвергенция технологий, информационное общество, робототехника*

DOI: 10.36535/0548-0019-2022-03-1

НЕГАТИВНЫЕ ТЕНДЕНЦИИ РАЗВИТИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Устойчивые тенденции быстрого развития телекоммуникационных и информационных технологий создали предпосылки появления широкого круга принципиально новых возможностей для получения информации и её расширяющегося использования в экономике и социуме. Уже сейчас можно констатировать максимально широкое «вплетение» цифровых информационных технологий в ткань любых производственных, технологических, образовательных, управленческих и общественных процессов. На основе глобальной сети Интернет создается единая цифровая среда (инфраструктура) с подключением к ней машин и оборудования, объектов инфраструктуры, транспорта, логистических цепочек, а также людей и организаций. Началом новой, информационной эпохи и глобализации как ее непосредственного выражения считают 1991 г., когда в США расходы на приобретение информации и информационных технологий превысили затраты на производственные технологии и основные фонды [1].

Глобализация как высший этап интеграции – это процесс формирования и развития единого общемирового финансово-информационного пространства вследствие предельного упрощения коммуникаций на базе информационно-компьютерных технологий [2]. По мере развития процессов глобализации, исчерпания ресурсов, сокращения рынков сбыта, перепроизводства и постоянного сокращения платежеспособного спроса (особенно на высокотехнологичную продукцию) информационные технологии сделали наиболее рентабельным видом деятельности не традиционное преобразование окружающего мира, а формирование (преобразование) самого человеческого сознания (как индивидуального, так и коллективного) посредством коммерческой рекламы, политической пропаганды, методов социальной инженерии [3]. В мировой экономике кризисные процессы проявляются прежде всего в нехватке спроса: как на производимые товары и услуги (т.е. кризис перепроизводства), так и на продукцию, намеченную к выпуску на рынок реализуемыми инвестиционными проектами (кризис переинвестирования). Спрос – главный дефицит глобализируемой рыночной экономики. С эскалацией процессов глобализации наблюдается смена вектора-парадигмы развития человечества – переориентация технологического прогресса с создания новых технологий производства на создание технологий целевого формирования сознания для возникновения новых потребностей человека и, соответственно, новых рынков, позволяющих продлить существование рыночной экономики. Именно эти процессы манипуляции сознанием человека (сообществ, социальных групп) потенциально содержат в себе континиум социальных *мега рисков* для будущего развития человечества.

Исторический ход научно-технического развития показал невозможность предвидеть весь спектр его негативных последствий для человечества. С процессами формирования нового технологического уклада на базе информационных технологий связана фундаментальная неопределенность, поскольку общество, во-первых, просто не готово к столь масштабному расширению пределов возможного, а во-вторых, уже явные возможности влекут за собой и опасные последствия, большинство из которых все еще относится к сфере незнания. Следует отметить возрастание актуальности исследований негативных последствий научно-технического и индустриального развития, так как проблема минимизации *рисков* внедрения новых технологий является частью более общей проблемы социального и научно-технического развития [4-9]. Современные представления о риске отличаются многообразием (особенно в финансово-экономической сфере) [10]. В рамках данной статьи используется термин «*мега риски*» вследствие потенциальной значимости и масштабности негативных последствий развития информационных технологий в виде: перестройки общественных отношений, атомизации общества, трансформации и деградации личности, корректировки культурного кода наций, нарастания цифрового неравенства и информационной конфронтации, роста международного терроризма, снижения значимости знания.

Цель статьи – проанализировать и структурированно показать ограниченный пул наиболее значимых угроз и *рисков* развития и использования информационных технологий, актуальных для мирового социума в период глобализации рыночной экономики.

СТРУКТУРНЫЙ АНАЛИЗ ПОТЕНЦИАЛЬНЫХ УГРОЗ И РИСКОВ ИНФОРМАТИЗАЦИИ

По мере развития цифровой экономики, особую важность и актуальность приобретает проблема (междисциплинарная по своему характеру) выявления и оценки уровня угроз и *рисков* применения новых информационных технологий для жизни современного общества и цивилизации в целом. Технологический

риск понимается по-разному не только в различных областях, но и в рамках одной области техники [11]. Причем *риски* применения новых технологий часто не осознаются сразу и требуется определенный период времени для выявления точек *риска*. В особенности это относится к новейшим информационным технологиям, часто первоначальное эйфорическое отношение к которым по прошествии определенного времени сменяется резко критическим осознанием последствий их применения и, главное, социальной и психологической зависимости от них. Прагматически существенным и важным является исследование и раннее распознавание (прогнозирование) таких угроз и *рисков*, причины и/или следствия которых имеют системный характер или же характеризуются синергетическими эффектами. Раннее распознавание в когнитивном отношении характеризуется следующими шагами: идентификация проблемы, ее концептуализация, селекция и анализ информации, интерпретация и оценка результатов. В короткой статье невозможно уделить достаточного внимания всему множеству {IT-рисков}. Однако с позиций системного подхода, применения методов наукометрии (понимаемых расширительно), многомерного и сопоставительного анализа представляется возможным выделить следующие, наиболее значимые, с точки зрения формирования безопасного (в широком смысле) информационного общества, *риски* развития информационных технологий. В последующих подразделах настоящей статьи анализируются причинно-следственные связи возникновения новых, наиболее опасных и значимых угроз и *мега рисков* {A,B,C,D,E,F,G,H,I,K} для экономики и социума, зачастую не вполне осознаваемых даже в профессиональном сообществе.

A. В последнее время все более начинает осознаваться относительно новый, и безусловно самый опасный, вид угроз – разрушение способов и форм идентификации личности в результате длительного информационно-психологического воздействия, что влечет переструктуризацию (трансформацию) внутреннего мира личности. С развитием информационных технологий, в том числе технологий Big Data (Больших Данных), ростом сетевого пространства, успехами социальной инженерии, когнитивных и поведенческих наук, возрастают *риски*, обусловленные целевым негативным воздействием на сферу общественного сознания, что проявляется в виде деструктивной социальной трансформации. Доминирующие тренды – формирование личности не относительно глубокими переживаниями, связанными с непосредственно прожитыми реальными событиями, а переживаниями достаточно поверхностными, связанными с потреблением готовых эмоций, предоставленных электронными СМИ, соцсетями и платформами. Непосредственное, хаотичное и без усилий (которое и формируют устойчивые структуры личности) потребление эмоций из сети делает современную информатизированную личность не только пластичной, но и мозаичной: способной одновременно испытывать разные чувства и давать противоположные оценки одним и тем же событиям. Зависимость от эмоций приобретает наркотический (отсюда широкое распространение игромании и зависимости от соцсетей и платформ), причем поверхностный, неглубокий характер поставляемых в готовом виде эмоций, создает потребность в их постоянном обновлении и формировании «клипового» сознания (разорванность причинно-следственных связей, неспособность и нежелание их выстраивать, фрагментарность и ограниченность восприятия, внушаемость и отсутствие критического мышления). Исследователи из Института сложности в Санта-Фе установили, что клиповый тип мышления на порядок повышает внушаемость людей [12]. В 2016-2017 гг. до 70% граждан США и более 80% Евросоюза удовлетворялись уже освоенными, постоянно посещаемыми ими ресурсами Интернета и соцсетей и лишь пассивно потребляли информацию, не расширяя зону своего внимания [13]. В [12] отмечается, что принудительное сужение поисковиками и платформами когнитивного разнообразия пользователей в погоне за их вниманием ведёт к социальной инстинктивизации (и примитивизации), вырабатывает автоматизм и усиливает стереотипы поведения. Как экспериментально показал российский нейропсихолог и нейрофизиолог С.В. Савельев, автоматизация познавательной поведенческой активности ведет к морфологическим изменениям в головном мозге [14]. Вследствие высокой пластичности мозга церебральное закрепление алгоритмического поведения может происходить в значительно более сжатые временные периоды, чем считалось ранее [15].

Трансформация личности под воздействием информационных технологий дополняется воздействием разнообразных лекарственных средств в их никем не изучаемых сочетаниях (на пример при COVID-19). Следующим этапом трансформации личности может стать распространение медицинских (мозговых) имплантов, объединенных в сеть и частично управляемых по Интернету. В 2013 г. в США было продано 12 млн привязанных к Интернету имплантов, большинство из которых решало локальные физиологические задачи (контроль за деятельностью сердца, предупреждение воспалений, блокирование боли) [16]. Массовое использование имплантов (например, для стимулирования мозговой деятельности) и прямой доступ к Интернету представляется близким будущим, которое не только ускорит, но и откорректирует изменение личности.

Все это, в итоге, ведет к росту рисков деградации личности и целенаправленного негативного воздействия современной цифровой сетевой среды (инфосферы) на когнитивные способности, мотивацию, целеполагание и поведение людей.

B. Развитие информационных технологий предопределяет сознательное подстегивание человеком своей биологической эволюции при помощи социальных платформ и генной инженерии. Биологическая эволюция человека уже сегодня значительно меньше определятся внешними для него факторами, чем внутренними – технологиями и социальной структурой, преобразующими по его интересам и потребностям уже не только окружающий мир, но и его самого. В перспективе весьма вероятной следует рассматривать актуализацию *рисков*, связанных с конвергенцией биомедицинских и компьютерных техно-

логий. В интервале 15–25 лет синтетическая биология, генетическая инженерия, практическое применение нанороботов, способных действовать внутри кровеносной системы человека, совершенно поменяют лицо медицины. На горизонте 15–25 лет реальностью станет биотехнологическая интеграция человека и искусственного интеллекта, формирование своего рода биокибергов. Представление о том, что искусственный интеллект превзойдет человека – это упрощение сложного феномена. Психика человека, его интеллект работает одновременно в трех сферах: цифровой, аналоговой (или модальной) и образной. Воображение, распознавание закономерностей и сложные формы коммуникаций – это когнитивные области, где у людей до сих пор имеется неоспоримое преимущество, которое наверняка сохранится и в будущем. Многие специалисты и футурологи считают, что таким образом «синтезированные люди» будут обладать высокими креативными способностями, крепким здоровьем и высокой трудоспособностью в течение многих десятков и, возможно, сотен лет [13]. Это будет новый вид людей, живущих в полной реальности, включая цифровую и дополненную, здоровых и работоспособных от рождения до смерти. Этот новый человеческий вид будет неразрывно связан с искусственным, вычислительным интеллектом (прямой интерфейс мозг–компьютер), базами данных различного целевого назначения, системами поддержки принятия решений и распознавания.

Развитие синтетических технологий создания биокибергов (суперлюдей) неизбежно трансформирует современную человеческую цивилизацию, т.е. возникнет новая, нечеловеческая цивилизация с непредсказуемыми рисками и, возможно, глобальными негативными последствиями для антропосферы (ноосферы) в целом.

С. Информационные технологии увеличивают количество информации ее прямым порождением, зачастую без участия физического мира. Значимым следствием все более широкого использования цифровых данных и применения информационных технологий является формирование качественно новой информационной среды жизнедеятельности человека, дополняющей привычные сферы существования (естественную и техногенную). Антропогенная нагрузка приблизилась к объективному пределу, и человек начинает решать проблему приспособлением себя к окружающей среде. Возникновение и развитие современного информационного общества осуществляется на основе этой новой, виртуальной, информационной среды, базирующейся на принципиально новых элементах социальной инфраструктуры в виде электронных СМИ, социальных сетей, эволюционирующих в социальные платформы, влияющие на ментальность и поведение их участников. Управление сознанием и поведением, как массовым (в преломлении теории Гюстава Лебона [17]), так и индивидуальным, через управление массмедиа и соцсетями обычно сопровождается незаметным для самого человека принятием системы ценностей, нужных управляющей системе, что влечет глубокое и комплексное преобразование личности. Социальные сети как структурообразующий элемент общества трансформируются в социальные платформы, катализирующие активность личности и определяющие ее поведение через информационно-эмоциональный фон. Внешнее воздействие через формирование эмоционально-информационной среды существования в соцсетях индивидом, как правило, не ощущается. Человек воспринимает эту искусственно созданную среду как естественную, единственно объективную, отражающую реальное устройство мира и социума. Следует отметить, что влияние на человека социальных платформ более эффективно, чем соцсетей, так как их функционирование связано с процессами в реальном мире, и поэтому связанная с ним информация закрепляется в сознании сильнее. Эффективные социальные технологии, массмедиа и социальные платформы являются мощным инструментом управления и целевого воздействия как на человека, так и на отдельные сообщества и социальные группы. Современная социальная инженерия – это более эффективный инструмент, чем финансы и войны. Информационные технологии, атомизируя социумы, способствуют трансформации общественных отношений. При целевом длительном воздействии возможна корректировка культурного кода целых народов (например, в странах Прибалтики и на Украине). Появляются эффективные разработки, ориентированные на неявный сбор данных и скрытое управление групповым поведением коллективов большой размерности [8, 18]. Современные тенденции в области обработки данных (с расширенными возможностями многомерного статистического анализа) свидетельствуют о том, что в ближайшем будущем нас ожидает этап концентрации информационных ресурсов в больших суперкомпьютерных системах (центрах) нового поколения (технологии Больших Данных). Здесь следует упомянуть китайскую государственную «систему социального рейтинга», реализуемую с 2015г. Эта система осуществляет комплексную оценку поведения личности на основе всеобъемлющего и непрерывного мониторинга огромных массивов прямых и косвенных признаков, собираемых и обобщаемых в рамках технологии Больших Данных (а также реализует перечень санкций для обладателей низкого социального рейтинга) [19]. Суперкомпьютерные технологии позволяют автоматически сегментировать и обрабатывать огромные объемы информации. Суммируя полученный контент и выделяя в нем ключевые смысловые группы, можно получить информацию в различных разрезах об интересах и настроениях всех субъектов исследуемого сегмента. Анализ всего объема данных позволяет определять, какие настроения и ценностные ориентации преобладают в исследуемом социальном сегменте и, следовательно, каким образом информационно можно проникнуть в это сообщество (в том числе с использованием СМИ), с какими смысловыми и мировоззренческими посылами можно формировать нужный контекст в том или ином государстве. Поведение общества (или крупных социальных групп) внутри государства становится инструментальным фактором, на который можно воздействовать извне, тем самым формируя как внутриполи-

тическую повестку, так и поведение государства на внешнеполитической арене. Таким образом управление сознанием с использованием информационных технологий и методов социальной инженерии становится эффективным средством воздействия, за которым следуют социальные трансформации и, зачастую, реальные геополитические изменения.

В целом следует констатировать, что информационные технологии перманентно являются (в структуре рыночной экономики) источником мультипликативных рисков целенаправленного изменения индивидуального и общественного сознания, поведенческих предпочтений больших групп, трансформации социальной структуры – посредством использования активных методов (в том числе психометрических алгоритмов), деструктивных социальных сетей, новых технологий мультимедиа и виртуальной реальности.

D. Возрастающая интеллектуализация производства и ускорение прогресса резко повысили роль не только интеллекта, но и его знаний (точнее информации, которой он оперирует). Информация стала главным определяющим фактором не только управления, но и производства. Технология ее обработки превратилась в ключевое направление развития, породившее и современные информационные технологии, и саму информационную революцию, признаком которой является взрывообразное ускорение роста количества информации. Новая цифровая информационная среда, ее коммуникативная система способствует усложнению, саморазвитию, самопорождению информации, усилению ее влияния на материальный мир. Взрывообразное увеличение количества информации влечет за собой взрывообразное расширение воспринимаемого человечеством мира. Человек эпохи информационной революции живет в физическом мире, но действует на основе представлений виртуального информационного мира, которые все больше отдаляются от мира физического. Этот ***нарастающий разрыв между представлениями (а следовательно, и мотивацией) и реальностью порождают риски снижения эффективности и адекватности в сферах управления, принятия решений, объективного продуктивного анализа, масштаб и разрушительность которых также растут.*** Человек создал мир (естественная, техногенная. информационная среда), слишком сложный для своего индивидуального интеллекта. Усложняя мир, информационные технологии снижают его познаваемость индивидуальным сознанием. Человек воспринимает информационный мир, живя в физическом. В результате он все больше реагирует не на тот реальный мир, в котором живет, а на виртуальный, утрачивая критерий истины. Отсюда обострение противоречия между ростом важности упорядочивания информации и технологической ограниченностью возможностей этого упорядочивания. Масштабы восприятия устойчиво превышают возможности сознания, продуктивного анализа, традиционных способов познания (прежде всего логического мышления) и начинают давать систематические сбои. В значительной степени, вследствие этого, наиболее перспективным направлением познания считается сейчас эмпирический поиск взаимосвязей в больших массивах информации (технологии Big Data) с принципиальным отказом от осмысления выявляемых причинно-следственных связей и нахождения их содержательного смысла.

Важным следствием расширения кругозора за пределы, доступные здравому смыслу, является фрагментарность анализа и, зачастую, отказ от логики в пользу интуиции. Логика (и соображения здравого смысла) уступает свое влияние эмоциям (что делает психологию важной частью принятия решений и управления).

Информатизация общества сделала наиболее важным не рутинный, а творческий труд. Интернет предоставляет людям равные возможности по доступу к неструктурированной и непроверенной информации. Быстрый рост производительности персональных компьютеров уравняет людей и по возможности использования логических операций. Широкое применение персональных компьютеров и изначальная интерактивность Интернета меняют соотношение между логическим сознанием, опирающимся на вторую сигнальную систему [20, 21], и сознанием эвристическим, творческим, опирающимся на непосредственно чувственное восприятие (в том числе вербальных сигналов) и образное (а не формально-логическое мышление). Это будет означать концентрацию усилий человека на недоступной компьютеру сфере мышления, в которой сохранится исключительная монополия *homo sapiens*, – мышлении внелогическом, образном (творческом). Соответственно, и конкуренция людей будет вестись на основе внелогического, образного мышления. Тенденция снижения значимости логического мышления в пользу внелогического, базирующегося на образах, уже создает ощутимые общественные проблемы [13]. Очевидные, нарастающие даже в единой культурной среде проблемы с коммуникациями представляют собой закономерные, а не случайные и сами собой преходящие явления. Причина проста: внелогическое мышление не имеет того единого универсального языка для взаимодействия разных типов сознания, которое дает логика (оно оперирует образами, а образы у каждого свои).

Риски деформации коммуникативной среды особенно значимы с учетом того исключительного значения, которое имеет язык для формирования и развития личности, а единый общественный язык – для ее социализации.

Исчезновение единого универсального языка может привести через некоторое время и к распаду основанной на нем второй сигнальной системы, что может иметь непредсказуемые негативные последствия (в том числе торможение научно-технического прогресса).

E. Процессы глобализации разделяют людей и общества по степени участия в создании и использовании информационных технологий и, соответственно, по их богатству. Вследствие быстрого развития сетевых и информационных технологий информационно-цифровое неравенство становится актуальной и динамической проблемой. Развитие информационно-коммуникационных технологий дает толчок интеграционным процессам в экономике и обществе, но в то же время усиливает процессы поляризации различных групп населения, регионов и стран. Возникает

опасность формирования новой «информационной элиты», а также увеличения определенной страты людей, оказавшихся в маргинальном положении по отношению к информационно-компьютерным технологиям. Основными факторами угроз, способствующими появлению информационно-цифрового неравенства, являются: недостаточно развитая информационно-коммуникационная инфраструктура; высокая стоимость компьютерного оборудования и интернет-услуг; низкий уровень развития образования и информационной культуры населения; отсутствие социальной поддержки в освоении информационных технологий; слабая мотивация и готовность разных групп населения к использованию информационно-компьютерных технологий [7]. В геополитическом плане процесс информатизации осуществляется крайне неравномерно и резко усиливает технологическую (и экономическую) стратификацию стран мирового сообщества. Выступая в качестве мощного катализатора научно-технического прогресса, информатизация существенным образом ускоряет развитие передовых стран, обрекая тем самым другие страны на всё большее отставание. Именно поэтому необходимо уже сегодня принимать меры по ослаблению негативных последствий развития глобальной проблемы информационного неравенства, так как информационное неравенство усиливает социальное расслоение общества и представляет угрозу для его стабильности.

Можно констатировать, что развитие цифровой экономики (в рамках рыночной парадигмы) неизбежно обострит проблему информационно-цифрового неравенства и, как следствие, проблему экономического неравенства, что будет приводить к возникновению угроз, обусловленных ростом социальной и политической напряженности.

F. Помимо проблем цифрового неравенства ***нарастают риски, связанные с цифровой зависимостью***. Современные технологии все больше ставят пользователя в положение дилера или лицензиата – об этом свидетельствует фактическое превращение интеллектуальной собственности в инструмент злоупотребления монопольным положением владельцев технологий, в первую очередь – информационных. В сегменте системного программного обеспечения (ПО), например, модификации последних лет широко используемой операционной системы *Windows* позволяют реализовать не только дистанционное обновление программного обеспечения, но и осуществлять внешнее управление (и доступ к информации без ведома пользователя) подключенным к Интернету компьютером. В этом сегменте отечественные продукты практически отсутствуют (не считая международного открытого ПО типа *Linux*) [22].

Из-за фактического отсутствия в России в настоящее время собственной микроэлектронной промышленности постоянным и высоким фактором риска в сфере энергетики, промышленности, телекоммуникаций является широкое применение импортной электронной элементной базы. Значительны риски, связанные с использованием в сложных системах и критических приложениях импортной микроэлектроники. По разным оценкам, до 75% реализуемого на мировом рынке программного обеспечения (в первую очередь, системного ПО – ОС и СУБД) и 85% процессоров производится компаниями под американской юрисдикцией. Ряд крупных IT-компаний встраивают в производимые чипы целевые закладки в интересах спецслужб. Принципиальные схемы и исходные коды «зашитого» в чипах программного обеспечения известны только фирме разработчику. По некоторым оценкам существует потенциально высокий уровень рисков нарушения функционирования для ~90% отечественных энергосетей (невосстановимое отключение системы, перехват управления энергосистемой и т.п.) как из-за атак компьютерных вирусов (типа *Dugu* или *Stuxnet*), так и от внешних несанкционированных действий, осуществляемых за пределами их возможного обнаружения и идентификации [10].

Вследствие этого, с высокой степенью вероятности можно прогнозировать, что по мере развития информационных технологий в экономике и социуме будут нарастать риски, обусловленные факторами цифровой зависимости.

G. С проблемами информационно-цифрового неравенства опосредовано связаны тенденции нарастания угроз международного терроризма. Являясь одним из определяющих факторов глобализации, информационные технологии, включая технологии формирования сознания, радикально меняют не только облик и образ действий человечества в целом, но и характер конкретных явлений, – включая терроризм. СМИ, и прежде всего массовое телевидение, – породили «терроризм в прямом эфире», который, опираясь на коммуникативные возможности электронных медиа и естественную тягу людей к сенсациям, стремится к устрашению и дезорганизации не только управляющей элиты, но и общества в целом. Международный терроризм все более приобретает информационный характер, что не меняет его сути. Отсутствие географических границ, трудно определяемая национальная принадлежность объектов сети, возможность анонимного доступа к ее ресурсам – все это повышает уровень уязвимости общественной и личной безопасности. Возросшая эффективность психологического воздействия (и безнаказанность) делает «терроризм в прямом эфире» более доступным и массовым, превращая его в инструмент политического и экономического давления, в фактор глобальной нестабильности. Фундаментальные причины этого явления вполне объяснимы. Неразвитые общества лишаются приемлемых перспектив развития, а глобальные медиа, стремящиеся устранить культурные барьеры на пути распространения информационных технологий, насаждают высокие стандарты потребления, характерные для развитых стран. Это порождает в неразвитых обществах глубокую и безысходную неудовлетворенность. Их население в целом враждебно ценностям (и культуре) развитых стран, так как, все полнее (в силу формирования единого информационного пространства) знакомясь с этими ценностями, все острее сознает их недоступность для себя и своих детей. Вследствие нарастающего технологического разрыва увеличивается доля людей (в первую очередь молодых), осознающих отсутствие

для себя социальных перспектив. Вызванное этим отчаяние закономерно порождает озлобление и враждебность к развитым странам (а также стимулирует процессы нарастания массовой миграции) [8, 13, 23, 24]. Таким образом, терроризм имеет неистребимые в среднесрочной перспективе социально-экономические корни в развивающихся странах, численность населения которых во много раз превышает численность населения развитых стран. Здесь следует отметить, что население США составляет 4% мирового населения, а потребляют США 40% мирового продукта [25].

Вследствие этого можно прогнозировать, что с возрастанием информационно-экономического неравенства будут повышаться и риски нарастания террористической активности, глобальной социальной нестабильности и политической напряженности.

H. Широкое применение современных информационных технологий потенциально создает предпосылки таких угроз, как утечки, хищения, утраты, искажения, подделки, копирования и блокирования информации и, как следствие – экономического, экологического, социального и других видов ущерба [7, 26]. В разных странах регулярно регистрируются попытки несанкционированного проникновения в информационные системы органов государственной власти и управления, факты кражи и уничтожения экономической и финансовой информации, программного обеспечения систем электронных платежей и т.д. Несанкционированно вторгаясь в компьютерные сети, нарушители способны не только копировать хранящуюся в них информацию, но и вводить в них вирусы, разрушающие прикладные (или системные) программы, которые срабатывают спустя определенное время (или при возникновении определенных условий), что значительно усложняет их обнаружение. Такие действия могут приводить к функциональному нарушению информационных систем, систем защиты критической инфраструктуры, объектов управления, возникновению социальной напряженности (например, в случае утечки и несанкционированного использования персональных данных, лжеминирования авиационного и железнодорожного транспорта и т.п.). Статистика киберугроз 2020 г. имела следующий вид: несанкционированное изменение ПО организаций на 10% больше, чем в 2019 г.; количество инцидентов (с использованием вредоносного ПО) на промышленных предприятиях увеличилось на 91% по сравнению с 2019 г.; количество атак на медицинские организации по сравнению с 2019 г. выросло на 91%; количество атак на промышленность увеличилось почти в два раза по сравнению с 2019 г. В атаках на организации основными векторами доставки вредоносного ПО остаются электронная почта (71%) и компрометация компьютеров, серверов и сетевого оборудования (24%), а в атаках на частных лиц хакеры отдают предпочтение электронной почте и веб-сайтам (по 32%) [27].

Реализация *рисков* в промышленных отраслях влечет за собой глобальные последствия. Например, в ходе атаки на инфраструктуру водоснабжения и канализации в Израиле хакеры планировали изменить концентрацию хлора в подаваемой в жилые дома воде, что привело бы к массовому отравлению, а инцидент с отключением электроэнергии из-за кибератаки в Индии сказался на работе фондовой биржи, больниц и транспортной системы нескольких городов. Предугадать возможность реализации самых страшных рисков и оценить масштаб последствий на объектах критически значимой инфраструктуры сложно, поскольку даже самые опытные специалисты не могут дать гарантию, что все предусмотренные защитные механизмы сработают как нужно.

Информационная безопасность фактически становится одной из характеристик информационных систем и технологий. С позиций информатики здесь следует выделить два аспекта. Во-первых, реализация функций защиты требует все увеличивающихся информационных и вычислительных ресурсов, что влечет временные задержки и снижение производительности поиска и обработки информации. Во-вторых, быстрый рост глобальной сети, количества компьютерных систем, лавинообразный рост цифровых данных объективно влекут возрастание *рисков* и различного рода угроз целостности информации.

Наряду с традиционными проблемами информационной безопасности специалисты отмечают тревожную закономерность быстрого нарастания рисков, связанных с тем, что отдельный человек или относительно малая группа может получить и даже разработать оружие массового поражения (например, программируемые биовирусы, кибероружие, нановооружение и др.). Следует отметить, что современные методы и средства компьютерного моделирования позволяют значительно сокращать цикл «исследование – разработка» (за счет виртуализации лабораторных исследований и натурных испытаний) [28-30]. По мере развития цифровой экономики физический объем ущерба, который теоретически способен нанести всего один человек или небольшая группа, становится все больше и больше (возможно возникновение COVID-19 из этой страты *рисков*).

С высокой степенью вероятности можно прогнозировать, что такие факторы, как внедрение новых информационных технологий (в том числе суперкомпьютинга и систем искусственного интеллекта), расширение мировой сети телекоммуникаций, развитие сети Интернет и электронных массмедиа будут все более актуализировать проблему роста как традиционных угроз, так и качественно новых рисков в экономике и социуме.

I. В настоящее время роботизация рассматривается как одно из ведущих направлений развития информационных технологий, оказывающее существенное влияние как на экономические, так и на социальные (общество в целом) процессы. По данным *IDC* (*International Data Corporation*) мировой объем продаж робототехники и сопутствующих сервисов к 2020 г. превысил 188 млрд долл., что в два с лишним раза превышает объем продаж в 2016 г. (91,5 млрд долл.) [31]. Промышленные роботы перестают быть прерогативой тяжелой промышленности или огромных фабрик. Коллаборативные роботы, которые должны взаимодействовать с людьми в совместной рабочей среде, помогли расширить корпора-

тивную клиентскую базу – теперь она включает также предприятия среднего и даже малого бизнеса, занимающиеся легким производством, обработкой материалов, реализацией продукции и т. д.

По прогнозам, среднегодовой темп роста рынка робототехники в период с 2019 по 2024 гг. составит 9,2–12% и достигнет 774 тыс. роботов в 2024 г. При этом США производят ~75% мирового выпуска роботов, оснащенных вычислительным интеллектом и способных к многофункциональной деятельности. По экспоненте растет число транспортных и бытовых роботов. По-видимому, единственной труднороботизируемой сферой выступают военные конфликты между людьми, да и то, скорее, как противоречащие законам робототехники. Однако на практике именно сегмент роботов для военного применения развивается наиболее динамично.

В цифровой экономике именно человек становится наиболее непредсказуемым, а значит ненадежным звеном автоматизированных производств. Уже в настоящее время роботы вызывают страх у рабочих, юристов, работников транспорта, торговли, представителей других профессий с повторяющимися операциями [32]. Международная консалтинговая компания *McKinsey* предсказывает, что около 20% рабочей силы по всему миру – или более 800 млн рабочих – могут потерять работу из-за автоматизации процессов [33, 34]. В будущем до 15 млн россиян могут лишиться работы, которая не требует серьезной квалификации, так как их профессия вымрет. Об этом заявил член комитета Государственной Думы РФ по труду, социальной политике и делам ветеранов Олег Шеин порталу «URA.RU» (04.08.2019). В этой связи следует отметить, что, несмотря на масштабность и важность проблемы, в научном сообществе в настоящее время не разрабатываются какие-либо подходы и методы оценки *рисков* и оценки (переоценки) ценности человеческого капитала с учетом трендов процесса роботизации хотя бы на период до 2025 г.

С учетом современных тенденций следует констатировать, что весьма динамично актуализируются риски, обусловленные ростом социальной напряженности (в различных социальных слоях) вследствие быстрого прогресса робототехники. Технологическая безработица уже в глобальной «повестке дня».

J. Основной тенденцией развития микроэлектроники является повышение степени интеграции микросхем (согласно известному закону Мура [35]). С эволюционированием микроэлектроники актуализируются проблемы, связанные с *риском* возникновения случайных компьютерных сбоев. С подобными аномалиями микроэлектронная промышленность начала сталкиваться ещё в 1970-х гг., когда интегральные схемы достигли критически малых размеров. Практически сразу стало очевидным, что источниками подобных сбоев являются высокоэнергетические частицы космического излучения (протон, фотон, нейтрино). Попав в интегральную схему, частица может полностью вывести её из строя, наведя в отдельных элементах схемы вторичную радиацию (однако в большинстве случаев частицы пролетают схему насквозь, не причиняя физического вреда). Чаще всего космические лучи изменяют потенциал ячеек памяти микросхемы, например, заменяя один бит информации с ноля на единицу. Этот эффект именуют как "расстройство одиночного события" – *SEU* (*Single-event upset*) [36]. В зависимости от того, где конкретно и какое воздействие частица оказала на микросхему, разнятся и последствия этого «одиночного сбоя». Программа может либо просто выдать критическую ошибку данных, либо автоматически перезагрузиться, попытавшись восстановить свою работоспособность, а может продолжить работать, выдавая уже ошибочные данные, чем может спровоцировать каскадный эффект набора ошибок. Значимых проблем не возникает, если эта программа будет изолирована в рамках локальной системы (инверсированный бит можно переписать на правильный). Реальные *риски* возникают если она открыта для общего доступа и будет служить источником данных для выполнения прочих программ или подпрограмм, отвечающих, например, за безопасное выполнение опасных для человека или общества процессов. Ситуация ещё больше усугубляется с уменьшением размеров интегральных схем. Так, в схемах, выполненных по технологии 22 нм, частота возникновения "одиночных эффектов" увеличена на порядок по сравнению со схемами, основанными на техпроцессе 130 нм. При размерности 22 нм одиночная космическая частица способна поражать уже не один, а сразу несколько логических элементов схемы. Частота случаев необратимого повреждения микросомы также резко возрастает [37-39].

Два примера иллюстрируют социально значимые случаи компьютерных сбоев из-за самопроизвольного изменения бита.

1. В 2003 г. во время голосования в Бельгии «однократное расстройство» вследствие воздействия ионизирующей частицы изменило один бит информации с «0» на «1», что присвоило кандидату дополнительные 4096 голосов, приплюсовав их к реальным 514 голосам.

2. В 2008 г. частица ионизирующего излучения изменила бит информации в блоке инерциальной навигации и управления полётом самолёта "Airbus A330", что привело к неверным данным об угле атаки, высоте и скорости полёта. Автопилот самолёта отреагировал на это резким рывком вниз такой силы, что 119 пассажиров получили травмы разной степени тяжести. Кроме того, ошибка вызвала каскадный отказ в работе нескольких бортовых систем, что не позволило безопасно продолжить полёт.

Риски возникновения нештатных состояний программного обеспечения и, следовательно, непредсказуемых ситуаций весьма вероятны и при использовании широко распространенного объектно-ориентированного программирования (ООП) [40–43], использующего языки C++, Java, C# (так называемые высокоуровневые языки программирования). ООП-код является недетерминированным. В отличие от функционального программирования, нет гарантий в получении одинакового вывода при одинаковых входных данных. «Использование ООП в долгосрочной перспективе — это бомба замедленного действия, которая может взорваться, когда кодовая база станет достаточно большой. ООП предоставляет разработ-

чикам слишком много инструментов и вариантов, не налагая правильных ограничений. ООП-код поощряет использование разделяемого изменяемого состояния, которое может быть небезопасно от раза к разу» [44]. Следует отметить, что широко известные авиационные катастрофы последних лет (*Boeing* 747, *SSJ*-100 и др.), по мнению многих специалистов и экспертов, связаны с использованием в современной авионике ООП.

С расширением сферы применения компьютерных систем можно прогнозировать, что из-за эффекта SEU и несовершенства методов верификации программного обеспечения, будут увеличиваться риски сбоев и отказов, критичных для процессов в экономике и социуме.

К. В настоящее время подавляющее большинство видов современного оружия базируется на IT-технологиях. Возрастают *риски*, обусловленные все более широким использованием цифровых технологий в сфере стратегических ядерных вооружений, а также в военно-космической области. Еще в 2017 г. американская *RAND Corporation* отмечала в своем докладе, что распространение гиперзвуковых ракет увеличит возможность стратегической войны. Зарубежные военные и научно-технические специалисты отмечают постоянно растущее влияние искусственного интеллекта (ИИ) на современные виды вооружений и военной техники, серьезно расширяющие их возможности и меняющие существующие концепции их использования в военных конфликтах. Количество направлений и способов применения искусственного интеллекта в военном деле будет только расширяться вслед за появлением новых идей и реализующих их технологий. При этом следует отметить, что разработка военных интеллектуальных систем не контролируется международными договорами и конвенциями.

Сегодня существуют три основные проблемы, влияющие на эффективность и целесообразность применения искусственного интеллекта. Во-первых, многочисленные зарубежные исследования и экспертные оценки говорят о недопустимости полного доверия системам с ИИ в вопросах самостоятельного применения оружия. Высказываются опасения, что ИИ потенциально способен выработать решение на нанесение упреждающего удара по целям противника, если он увидит возможность получения преимущества в результате такого удара. В исследовании, проведенном американской организацией "Рэнд корпорейшэн", подчеркивается опасность использования ИИ для принятия стратегических военных решений по причине отсутствия критического мышления у систем, обладающих ИИ, и их склонности к состязательности, что, в целом, может привести к неверной оценке обстановки [45]. Во-вторых, проблемой использования ИИ в системах военного назначения является его принципиальная уязвимость для специализированных атак на аппаратно-программное обеспечение. В отличие от традиционных кибератак, требующих для успешного осуществления наличия уязвимостей аппаратного и программного обеспечения (вызванных, как правило, недостаточной проработкой вопросов безопасности при создании или эксплуатации такого обеспечения), атаки на ИИ в основном используют врожденные ограничения, присущие таким системам. Под этим понимается принципиальная невозможность на уровне обычной, специально не подготовленной к конкретному виду атак системы, обладающей искусственным интеллектом, отделять реальные входные данные от фальсифицированных. Даже для современных, математически крайне сложных алгоритмов реализации ИИ, практически идеально работающих в нормальных условиях, незначительное, не определяемое для человеческого восприятия, но продуманное изменение входных данных (например, коррекция изображения) может приводить к ошибочному результату. Поскольку значение искусственного интеллекта в военной сфере определяется именно высокой скоростью обработки больших массивов разнородных данных, позволяющей существенно сокращать длительность цикла управления войсками и оружием, то обратной стороной такого процесса может оказаться катастрофическое ухудшение ситуации в случае принятия решений по неполным, неверным или, что еще хуже, сфальсифицированным исходным данным [46]. Потенциальный *риск* использования ИИ значительно возрастает в случае, если террористические организации завладевают интеллектуальной системой, которая располагает автономной связью с системами вооружения [47]. В-третьих, значимый фактор *риска* связан с тем, что существуют фундаментальные причины, в силу которых программное обеспечение большой сложности нельзя сделать настолько надежным, чтобы можно было не сомневаться, что не возникнут нештатные режимы и ситуации.

В целом о высоком уровне такого рода потенциальных угроз и *рисков* косвенно говорит тот факт, что, по появившейся информации, по решению руководства в Китае, начиная с 2007 г. проводится оцифровка массивов знаний, инженерной и конструкторской документации по всем ключевым технологиям и научным направлениям. Также КНР создает крупнейшую в мире базу семян и генного материала не только по сельскохозяйственным животным, птицам и рыбам, но и в целом генную библиотеку обитателей Земли [48]. По сути, с учетом ***рисков санкционированного и/или несанкционированного применения ядерного оружия,*** речь идет о беспрецедентном проекте создания хранилища знаний, технологий, биоматериалов, которое гипотетически может понадобиться выжившим после катастрофы китайцам.

С учетом рассмотренных факторов с уверенностью можно прогнозировать, что по мере все более широкого использования информационных технологий в сфере вооружений неизбежно будут расти цивилизационные мегариски экзистенциального характера (экзистенциальные *риски* – это события, которые приводят к полному уничтожению, либо к постоянному и серьезному снижению качества жизни людей [49]).

НЕКОТОРЫЕ ВЫВОДЫ И АКТУАЛЬНЫЕ ЗАДАЧИ

Современное общество становится полем перманентного экспериментирования с новыми информационными технологиями, следствия которого могут быть не только позитивными, но и негативными как для общества в целом, так и для отдельных его граж-

дан, которые поневоле становятся подопытными субъектами и объектами различных угроз и злоупотреблений. Перед современным обществом стоят жизненно важные задачи адаптации человека к условиям существования и деятельности в информационной среде, характер многофакторного и многоуровневого взаимодействия с которой претерпевает существенные изменения во всех сферах. Для их решения необходимо понимать информационные процессы в обществе, информационную сущность происходящих социально-экономических преобразований, причем все это на общем фоне смены доминирующих технологических укладов [50]. Следует констатировать, что общественная проблематика, связанная с информатизацией общества, информационной безопасностью, развитием информационных технологий, не является больше национальной, она становится проблематикой всего мирового сообщества. Этот факт накладывает особый отпечаток на обсуждение проблем информационной безопасности (в широком смысле этого слова) и ответственности ученых, инженеров и политиков за эту безопасность. В настоящее время становится все более очевидной необходимость разработки принципиально новых подходов, концепций, моделей по обеспечению взаимодействия человека с информационной средой.

По мнению многих экспертов [23, 51], одна из междисциплинарных сверхзадач XXI в. – это управление *мегарисками* и безопасностью сложных систем в экономике и социуме. Сформулируем некоторые выводы, рекомендации, первоочередные и наиболее актуальные задачи разработки проблемы рисков развития информационных технологий для экономики и социума.

1. Четкое осознание основных целей и задач: а) раннее предупреждение *рисков* новых цифровых технологий и их конвергентных вариантов; б) разработка методологии их многокритериальной оценки (по социально-экономическим сегментам); в) формирование рекомендаций и комплексных мер по минимизации *рисков* и улучшение основы поиска решений (с позиций междисциплинарного и трансдисциплинарного подхода).

2. Разработка методов классификации и систематизации *рисков* на основе таксономии. Потребность в таксономии в данном случае возникает из-за сложности предметной области, не позволяющей провести ее систематизацию на основе некоторой достаточно просто выводимой классификации объектов, её составляющих [52]. Роль таксономии *рисков* на этапах создания и реализации информационных технологий состоит в том, что она должна позволять разным категориям специалистов, экспертов, программистов оценивать риски в самых разных аспектах: а) по значимости потенциальных негативных последствий; б) по различным факторам *риска* (сложности, времени и др.); в) по структурным и функциональным составляющим; г) по категориям потерь.

3. Создание принципов, методов и рекомендаций по определению и оценке *рисков* на основе системного подхода, системного анализа, методов социотехнического проектирования, социальной инженерии, имитационного моделирования, теории «нечетких» множеств (с использованием технологии Big Data).

4. Организация международной системы сбора (и БнД), анализа и систематизации данных по реализовавшимся *рискам*, прежде всего связанных с управлением больших системотехнических комплексов (таких как Чернобыль, Фукусима, Шушенская ГРЭС, Суэцкий канал и т.п.). Международное сотрудничество и обобщение международного опыта, ознакомление с уже имеющимися результатами исследований в этой области, конструктивное взаимодействие и совместная работа с зарубежными междисциплинарными группами ученых по данной проблематике.

4. Мониторинг и исследования на постоянной основе всех аспектов взаимодействия человека с информационной средой, в том числе таких негативных политико-правовых (и культурно-этических) последствий информатизации:

- усиление социально-политического контроля над обществом и личностью;
- появление «компьютерного бюрократизма»;
- широкое распространение компьютерной преступности;
- информационные воздействия, деформирующие традиционные культуры, нормы морали и нравственности.

6. Активизация участия России в разработке международного законодательства и нормативно-правового обеспечения функционирования мировых открытых сетей. В сфере национального законодательства по проблемам информационной безопасности необходима разработка Кадастра с целью повышения качества принимаемых законодательных актов и обеспечения их непротиворечивости.

7. Обеспечение координации мер государственных ведомств по предотвращению угроз информационной безопасности в глобальных сетях, создание специализированной структуры для контроля трансграничного обмена. Защита информационного пространства России является одним из приоритетных направлений обеспечения национальной безопасности. Создание национального сегмента сети Интернет необходимо, оно экономически и стратегически обосновано. В РФ следует создать: а) свою ключевую инфраструктуру Интернета, включая национальные корневые сервера, национальную систему маршрутно-адресной информации; б) свои электронные компоненты, оборудование, системное программное обеспечение. В качестве примера здесь можно упомянуть российский аналог СУБД Oracle – платформу «1С:Предприятие 8» компании «1С».

ЗАКЛЮЧЕНИЕ

Информационное общество и лежащие в его основе технологии обладают огромным и уже бурно реализующимся потенциалом влияния на жизнь человека [53]. Информатизация, конвергенция компьютерных, телекоммуникационных технологий и мультимедиа обеспечивают принципиально новый уровень социально-экономического и цивилизационного развития. Является ли это влияние заведомо позитивным; помогает ли оно автоматически выходу на траектории устойчивого развития цивилизации; не содержит ли в себе развитие информационно-коммуникационных технологий дополнительных (новых) источников неустойчивости и угроз мировому сообществу (и наци-

ональной безопасности России)? Эти вопросы приобретают все большую актуальность в условиях устойчивых тенденций глобализации мировой экономики (и перманентного мирового экономического кризиса), бурного развития информационных технологий, электронных массмедиа и сетевой информационной среды.

СПИСОК ЛИТЕРАТУРЫ

1. Иноземцев В.Л. Расколотая цивилизация: системные кризисы индустриальной эпохи // Вопросы философии. – 1999. – № 5. – С. 3-18.
2. Практика глобализации: игры и правила новой эпохи / под ред. М.Г. Делягин. – Москва: «Инфа-М», 2000. – 344 с.
3. Фурсов А.И. На пороге нового мира – есть ли субъект стратегического действия? // Однако. – 2011 (9 февраля). – №№ 1-2(64-66). – 21 с. – URL: https://coollib.net/b/240625/read (дата обращения 31.10.21).
4. Bechmann G. Risk and Rationality in a Futureoriented Society // Rationality in an Uncertain World / eds. G. Banse, I. Hronszky, G. Nelson. – Berlin: Edition Sigma, 2005. – P. 59-75.
5. Lenk H. Global TechnoScience and Rensponsibility. Schemes Applied to Human Values, Technology, Creativity and Globalisation. – Berlin: LIT, 2007. – 189 p.
6. Горохов В.Г., Сюнтюренко О.В. Технологические риски: информационные аспекты безопасности общества // Программные системы и вычислительные методы. – 2013. – №4(5). – С. 344-353.
7. Сюнтюренко О.В. Социальные и экономические риски развития информационных технологий // Научно-техническая информация. Сер. 1. – 2012. – № 6. – С. 1–5; Syuntyurenko O.V. The Social and Economic Risks of the Development of Information Technologies // Scientific and Technical Information Processing. – 2012. – Vol. 39, № 2. – P. 113-116.
8. Сюнтюренко О.В. Сетевые технологии информационного противоборства и манипуляции общественным сознанием // Научно-техническая информация. Сер. 1. – 2015. –№ 10. – С. 1-7; Syuntyurenko O.V. Network Technologies for Information Warfare and Manipulation of Public Opinion // Scientific and Technical Information Processing. – 2015. – Vol. 42, № 4. – P. 205-210.
9. Сюнтюренко О.В., Гиляревский Р.С. Тенденции и риски развития сетевых технологий // Научно-техническая информация. Сер. 1. – 2021. – № 5. – С. 1-11; Suntyurenkoa O.V., Gilyarevskiia R.S. Trends and Risks of Network Technologies // Scientific and Technical Information Processing. – 2021. – Vol. 48, № 2. – P. 97–106.
10. Сюнтюренко О.В. Риски развития цифровой экономики: информационные аспекты // Научно-техническая информация. Сер. 1. – 2020. – № 5. – С. 1-10; Syuntyurenko O.V. The Risks of the Digital Economy: Information Aspects // Scientific and Technical Information Processing. – 2020. – Vol. 47, № 2. – P. 104-112.
11. Бехманн Г., Горохов В.Г. Социально-философские и методологические проблемы обращения с технологическими рисками в современном обществе (Дебаты о технологических рисках в современной западной литературе) // Вопросы философии. – 2012. – № 7-8. – С. – 127-136.
12. Ларина Е.С. Понимание алгоритмических обществ. Гибридный интеллект и его зомби // Свободная мысль. – 2017. – № 5. – URL: http://www.svom.info/entry/773-ponimanie-algoritmicheskih-obshestv-gibridnyj-inte/ (дата обращения 27.12.2021).
13. Делягин М.Г. Конец эпохи: осторожно, двери открываются! Том 1. Общая теория глобализации. Издание 12-е, переработанное и дополненное. – Москва: ИПРОГ, Книжный мир, 2019. – 832 с.
14. Савельев С. Управление мозгом человека. – URL: http://poznavatelnoe.tv/savelev_upravlenie_mozgom (дата обращения 23. 12.2021).
15. Норман Дойдж. Пластичность мозга: Потрясающие факты о том, как мысли способны менять структуру и функции нашего мозга. – Москва: ЭКСМО, 2019. – 215 с. – URL: https://www.nwk.su/assets/files/BOOKS/Норман% 20Дойдж.20%Пластичность% 20мозга.pdf .
16. Harari Y. Homo Deus: A Brief History of Tomorrow. – New York: Harper, 2017. – 580 p.
17. Лебон Г. Психология масс. – Санкт-Петербург: «Питер», 2016. – 222 с.
18. Бреер В.В., Новиков Д.А., Рогаткин А.Д. Управление толпой: математические модели порогового коллективного поведения. – Москва: ЛЕНАНД, 2016. – 168 с. (Серия «Умное управление»).
19. Делягин М.Г. Конец эпохи: осторожно, двери открываются! Том 2. Общая теория глобализации. Издание 12-е, переработанное и дополненное. – Москва: ПОЛИТИЗДАТ, Книжный мир, 2020. – 816 с.
20. Ходусов А.Н., Шуклин С.И. Виртуализация сознания и мышления как основа формирования профессионального менталитета будущего специалиста // Философия образования. – 2011. – № 2. – С. 45-52.
21. Человек-трансформер. – URL: https://zavtra.ru/blogs/chelovek-transformer (дата обращения 21.12.2021).
22. Российское программное обеспечение (Отечественное ПО) (tadviser.ru). – URL : https://www.tadviser.ru/index.php/ (дата последнего обращения 21.12.2021).
23. Ларина Е.С., Овчинский В.С. Час волка. Введение в хронополитику. («Коллекция Изборского клуба») – Москва: Книжный мир, 2019. – 416 с.
24. Как отключили Интернет в Сирии. – URL: d-russia.ru/otklyuchenie-strany-ot-internetaprecedent-byl.html (дата обращения 19.12. 2021).
25. Фурсов А. Виртуальные миры и еда из насекомых. Какое будущее строят глобальные элиты. – URL: https://zen.yandex.ru/media/govoritfursov/virtualnye-miry-i-eda-iz-nasekomyh-kakoe-buduscee-stroiat-globalnye-elity-andrei-fursov-61a8bb7e548e48235267b828?& (дата обращения 21.12.2021).

26. Хоффман Л.Дж. Современные методы защиты информации. – Москва: Советское радио, 1980. – 263 с.
27. Актуальные киберугрозы: итоги 2020 года. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020/ (дата последнего обращения 17.12.201).
28. Компьютерное моделирование биотехнологических процессов и систем. – URL: https://knowledge.allbest.ru/programming/3c0b65635a2bd79a5c43a88421216d27_0.html (дата обращения 18.12.2021).
29. Как цифровое моделирование сокращает время и расходы на разработку новых моделей. – URL: http://www.dealeron.ru/news/4057 (дата обращения 21.12.2021).
30. Моделирование – в массы. – URL: https://habr.com/ru/company/dell_technologies/blog/406841/ (дата обращения 20.12.2021).
31. IDC: мировой рынок робототехники к 2020 году вырастет до 188 миллиардов долларов – URL: https://www.computerworld.ru/news/IDC-mirovoy-rynok-robototehniki-k-2020-godu-vyrastet-do-188-milliardov-dollarov (дата обращения 21.12.2021).
32. Бриньолфсон Э., Макафи Э. Вторая эра машин. Работ, прогресс и процветание в эпоху новейших технологий / пер. с англ. П. Миронова. – Москва: АСТ, 2017 – 384 с.
33. Промышленные роботы. – URL: www.tadviser.ru/index.php/Статья: Промышленные роботы (дата обращения 19.12.2021).
34. Международная федерация робототехники представила список самых роботизированных стран мира. – URL: https://rb.ru/story/countrits-withgreae (дата обращения 21.12.2021).
35. Закон Мура. – URL: https://www.tadviser.ru (дата последнего обращения 29.11.2021).
36. Расстройство единичного события – Single-event upset – Википедия (wikichi.ru). – URL: https://wikichi.ru/wiki/Single-event_upset (дата обращения 21.12.2021).
37. O'Neill P.M., Badhwar G.D. Single event upsets for Space Shuttle flights of new general purpose computer memory devices // IEEE Transactions on Nuclear Science. – Oct. 1994. – Vol. 41, № 5. – P. 1755-1764. DOI: 10.1109/23.317386. – URL: https://ve42.co/ONeill1994 (дата обращения 26.12.2021).
38. Carlson P., de Angelis A. Nationalism and internationalism in science: the case of the discovery of cosmic rays // The European Physical Journal H. – 2011. – Vol. 35(4). – P. 309-329. – URL: https://ve42.co/Carlson2011.
39. Höeffgen S.K., Metzger S., Steffens M. Investigating the effects of cosmic rays on space electronics // Frontiers in Physics. – 2020. – № 8. – P. 1-9. – URL: https://ve42.co/Hoeffgen2020 (дата обращения 26.12.2021).
40. Объектно-ориентированное программирование – самая большая ошибка компьютерных наук. – URL: https://proglib.io/p/obektno-orientirovannoe-programmirovanie-samaya-bolshaya-oshibka-kompyuternyh-nauk-2021-01-23?utm_referrer=https%3A%2 (дата обращения 22.01.21).
41. Почему ООП — это плохо. – URL: https://yandex.ru/turbo/ru.hexlet.io/s/blog/posts/pochemu-oop-eto-ploho (дата обращения 02.04.21).
42. Прощай, объектно-ориентированное программирование. – URL: https://webdevblog.ru/proshhaj-obektno-orientirovannoe-programmirovanie/ (дата обращения 04.02.2021).
43. Почему объектно-ориентированное программирование провалилось? – URL: http://citforum.ru/gazeta/165/ (дата обращения 04.02.2021).
44. Мнение: объектно-ориентированное программирование – катастрофа на триллион. – URL: https://tproger.ru/translations/oop-the-trillion-dollar-disaster (дата обращения 04.02.2021).
45. Искусственный интеллект в военном деле. – URL: https://arsenal-otechestva.ru/article/1503-iskusstvennyj-intellekt-v-voennom-dele (дата обращения 21.12.2021).
46. 46. Основные направления применения искусственного интеллекта в вооруженных силах ведущих зарубежных стран. – URL: https://zavtra.ru/books/osnovnie_ napravleniya_primeneniya_iskusstvennogo_intellekta_v_vooruzhennih_silah_vedushih_zarubezhnih_stran (дата обращения 21.12.2021).
47. Torres P. Agential Risks: A Comprehensive Introduction. – URL: https:// jetpress.org/v26.2/torres.pdf (дата обращения: 22.12.2021).
48. В Китае создают силиконовую долину семян. – URL: https://agroportal.ua/news/mir/v-kitae-sozdayut-silikonovuyu-dolinu-semyan/ (дата обращения 22.12.2021).
49. Экзистенциальные риски и неконтролируемая цифровая эволюция (texterra.ru). – URL: https://texterra.ru/blog/ekzistentsialnye-riski-i-nekontroliruemaya-tsifrovaya-evolyutsiya.html (дата обращения 19.12.2021).
50. Родионов И.И., Гиляревский Р.С., Цветкова В.А. Информационная деятельность как инфраструктура национальной экономики. – Санкт-Петербург: Алетея, 2016. – 223 с.
51. Малинецкий Г.Г. Сценарии, стратегические риски, информационные технологии // Информационные технологии и вычислительные системы. – 2002. – № 4. – С. 83-108.
52. Метод структурной таксономии: возможности применения для анализа социальных и духовных процессов. – URL: https://cyberleninka.ru/article/n/metod-strukturnoy-taksonomii-vozmozhnosti-primeneniya-dlya-analiza-sotsialnyh-i-duhovnyh-protsessov (дата обращения 22.12.2021).
53. Родионов И.И., Гиляревский Р.С., Цветкова В.А. Неоинформационная экономика и ее общество. Тенденции развития. – Москва, 2021. DOI 10.36535/978-5-600-02928-6.

Материал поступил в редакцию 13.01.22.

Сведения об авторе

СЮНТЮРЕНКО Олег Васильевич – доктор технических наук, профессор, главный научный сотрудник ВИНИТИ РАН, Москва
e-mail: olegasu@mail.ru

ОРГАНИЗАЦИЯ ИНФОРМАЦИОННОЙ РАБОТЫ

УДК 005.32:331.101.3

Л.В. Астахова

Модель нулевого доверия как фактор влияния на информационное поведение сотрудников организации*

Охарактеризована устойчивая тенденция к использованию концепции и модели нулевого доверия (zero trust) в мировой практике обеспечения информационной безопасности, выявлены проблемы ее реализации пользователями информационных систем. Обосновано негативное влияние этого подхода на информационное поведение сотрудников организации. Показана необходимость совершенствования модели нулевого доверия для устранения и предупреждения инцидентов угрозы информационной безопасности по вине пользователей и возможность использования в этих целях эвристического потенциала теории культуры информационной безопасности, теории доверия и теории самодетерминации.

Ключевые слова: *нулевое доверие, «zero trust», информационная безопасность, повышение осведомленности, культура информационной безопасности, теория самодетерминации, культура доверия, сотрудник, организация*

DOI: 10.36535/0548-0019-2022-03-2

ВВЕДЕНИЕ

Количество* инцидентов угрозы информационной безопасности (ИБ) в мире продолжает расти. В 2020 г. специалисты Экспертно-аналитического центра компании InfoWatch зафиксировали 2395 утечек данных из коммерческих и некоммерческих (государственных, муниципальных) организаций в различных странах мира (что на 5,8% превышает показатели 2018 г.), а также рост количества умышленных утечек [1]. Инсайдеры – самые частые виновники инцидентов. По оценкам компании SearthInform, в первом полугодии 2020 г. как минимум 60% утечек данных в России произошло по причине намеренных действий сотрудников организаций, которые имели к ним доступ [2]; ежемесячно каждая организация выявляла не менее 25 инцидентов по вине сотрудников и столкнулась с попытками слива информации [3]. Стабильно не снижающиеся цифры подобных инцидентов заставляют теоретиков и практиков в области ИБ искать новые концепции, подходы и модели их устранения.

Все большее внимание привлекает модель «нулевого доверия» (*zero trust*), призванная удовлетворять новые сложные требования сетевой безопасности организаций. Эта модель, разработанная в 2010 г. Дж. Киндервагом [4], стала наиболее популярной в сфере кибербезопасности как в России, так и за рубежом. Ее суть заключается в полном отсутствии доверия кому-либо – даже пользователям информационных систем организации. Подразумевается, что любой пользователь или устройство должны подтверждать свои данные каждый раз, когда они запрашивают доступ к какому-либо ресурсу внутри или за пределами сети. К основным принципам нулевого доверия авторы [5] относят: причисление всех источников данных и вычислительных услуг к организационным ресурсам; запрет на автоматическое предоставление доверия по умолчанию; доступ к ресурсам только на один сеанс; определение доступа исходя из характеристик устройства, поведенческих атрибутов; применение наименьших привилегий; постоянное обновление и оценку доступа; сбор и использование информации об активах, сетевой инфраструктуре и сообщений для улучшения безопасности. Несмотря на актуальность и широкое распространение этой модели и учитывая статистику роста инцидентов угрозы ИБ по вине внутренних пользователей, можно выразить сомнение в ее результативности. Этим обусловлена актуальность и цель настоящей статьи –

* Статья подготовлена при поддержке Правительства РФ (Постановление № 211 от 16.03.2013 г.), соглашение № 02. А03.21.0011.

выявить проблемные векторы влияния нулевого доверия на информационное поведение сотрудников организации и обосновать пути их коррекции.

ПОЛЬЗОВАТЕЛЬ ИНФОРМАЦИОННОЙ СИСТЕМЫ В МОДЕЛИ НУЛЕВОГО ДОВЕРИЯ КАК ОБЪЕКТ ИЗУЧЕНИЯ

Результаты исследований показывают, что в академической литературе основное внимание уделяется архитектуре ИБ и повышению её производительности при нулевом доверии, а в практической литературе – организационным преимуществам модели нулевого доверия и потенциальным стратегиям её развития. Однако и научные круги, и практики до сих пор игнорируют исследования пользователей в контексте *zero trust* [6]. При этом встречаются публикации, в которых декларируется роль пользователей как одного из наиболее слабых звеньев концепции угрозы безопасности и необходимость ограничить и контролировать их доступ к ресурсам внутри и вне компании [7]. Эксперты констатируют факт невнимания к пользователям в ходе внедрения модели «нулевого доверия», указывают, что возможные проблемы могут привести к их недовольству [8], и рекомендуют проводить предварительную загрузку и автоматическое обновление настроек, предоставлять краткие объяснения причин отказа в доступе. А для того, чтобы минимизировать разочарование пользователей с самого начала, призывают предвидеть потенциальные конфликты и проблемы и принимать меры реагирования [9]. На вопросы влияния нулевого доверия на взаимодействие человека и компьютера, человека и внешнего мира эксперты ответов не находят. Неясными остаются и возможности атак изнутри сети с нулевым доверием [10]. Как ни парадоксально, в процессе разработки этой новой модели специалисты-практики не обращаются к пользователям как к ее ключевому элементу, чтобы максимально учесть их потребности. В результате спустя десять лет по-прежнему существуют человеческие риски, которые несет построение в компании такой системы безопасности [11]. И в первую очередь к ним относят уклонение персонала от норм ограниченного доступа к данным и возникновение организационно-коммуникационных трудностей, связанных с ограничением доступа пользователей к информации.

Если иметь в виду человека, то мы не можем не рассматривать эту проблему в гуманитарной плоскости. Очевидно, что названные риски возникают не только по причине низкой осведомленности об ИБ сотрудников организации, но и из-за негативного влияния нулевого доверия на психологическую сферу личности сотрудника, на его информационное поведение.

Мы выделяем два вектора влияния нулевого доверия на пользователя информационной системы организации – позитивный и негативный.

Позитивное влияние модели нулевого доверия выражается в активном развитии практики повышения осведомленности сотрудников организации в области ИБ, необходимость которой ещё в начале XXI в. приходилось доказывать как проявление гуманитарной сущности деятельности по обеспечению ИБ [12]. Сегодня эта практика закреплена в международных и национальных стандартах по управлению информационной безопасностью, в нормативных правовых документах по защите персональных данных, критической информационной инфраструктуры и др. И это, безусловно, позитивный факт. Куда более сложен негативный вектор влияния нулевого доверия на информационное поведение сотрудников. Он связан со снижением доверия пользователей к руководству и внутренней мотивации к выполнению правил ИБ организации.

Снижение доверия пользователей к работодателю. Контроль со стороны руководства (нулевое доверие) часто воспринимается пользователями информационной системы как недоверие. Гипертрофированный контроль и надзор, поведенческий мониторинг с помощью систем видеонаблюдения и DLP-систем (Data Leakage Prevention – предотвращение утечки данных) на рабочих местах могут порождать ответное недоверие (нулевое доверие), злобу и цинизм сотрудников, дегармонизировать взаимодействие в организации, приводить как к утечке инсайдерской информации, так и к активизации текучести кадров. При внедрении модели нулевого доверия авторы обращают внимание на проблему, которая заключается в том, что сотрудники могут чувствовать себя проверяемыми и контролируемыми [13]. Беспокойство экспертов вызывают постоянный мониторинг и проверка трафика, проблемы с конфиденциальностью данных сотрудников [14], связанные с правовыми нормами.

В своих публикациях мы уже уделяли внимание проблеме доверия в информационной безопасности [15, 16]. Анализ этой проблемы дает ключ и к решению негативного восприятия модели нулевого доверия в организации. Доверие – это информационно-измерительный механизм управления (планирования, реализации, контроля и мотивации) безопасным взаимодействием субъектов информационных отношений, направленным на их устойчивое функционирование и развитие. Поэтому контроль и мотивация пользователя – это важнейшие элементы, от сбалансированности которых зависит результативность любой модели информационной безопасности, в том числе – нулевого доверия.

Обосновав онтологический статус доверия в ИБ, требование баланса недоверия (контроля) и доверия, мы пришли к необходимости развития культуры доверия в информационной безопасности. Это - «способ организации человеческой деятельности, при котором субъекты информационных отношений способны управлять своими информационными взаимодействиями, направленными на их устойчивое функционирование и развитие в условиях информационных рисков, *посредством взаимного субъективного авансирования веры в ценности культуры и объективных действий по их передаче*» [15]. Взаимность авансирования веры в ценности культуры не требует исключительного доверия или недоверия друг к другу. Работодатель и сотрудник как субъекты информационных отношений должны стремиться к культуре доверия, основанной на балансе взаимного доверия и недоверия (выраженного в контроле в разумных пределах).

Культура доверия как феномен, определяющий потребность сотрудника в адекватном информационном поведении в организации, не может формироваться в рамках повышения осведомленности об ИБ. Нормативные документы и практика отличаются сугубо прагматической направленностью, отсутствием мотивационно-рефлексивных, мировоззренческих аспектов, на что мы не раз обращали внимание [17]. В последние годы в развитых странах мира осознается ограниченность столь прагматичного подхода, поэтому резко увеличился поток публикаций по культуре информационной безопасности, развивается её социальная практика в самых разных отраслях деятельности. Культура доверия является органичной частью развития культуры информационной безопасности – следующего этапа после повышения осведомленности об ИБ. Это следует учитывать при разработке моделей нулевого доверия в организациях.

Снижение внутренней мотивации работников к информационно-безопасному поведению в организации. В процессе внедрения модели нулевого доверия с ее жестким инструктивным характером снижается и мотивация пользователей. Это можно объяснить с позиции теории самодетерминации (ТСД), авторами которой являются американские психологи Эдвард Л. Деси и Ричард М. Райан [18]. Теория самодетерминации (*self-determination theory* – SDT) – психологический подход к пониманию человеческой мотивации, личности и психологического благополучия человека. В последние два десятилетия наблюдается всплеск активности в исследовании и применении этой теории в различных областях деятельности, функционирует специальная организация для ее продвижения [19]. Теория подчеркивает важность трех основных психологических потребностей человека – автономии, взаимосвязи и компетентности.

Уникальность теории самодетерминации заключается в её акценте на автономии. Способность индивида к автономии рассматривается как самодетерминация. Многие ошибочно путают автономию с независимостью, самостоятельностью и индивидуализмом, но в ТСД автономия – это чувство воли по отношению к своим действиям [20]. Согласно концепциям жизненных целей и причинных ориентаций, автономия способствуют развитию внутренней мотивации, и именно автономная (а не контролируемая) ориентация позитивно соотносится с психологическим здоровьем и эффективным поведением человека. Преобладание внутренней мотивации над внешними целями приводит к большей результативности деятельности человека [21]. Авторы ТСД [22] подчеркивают, что автономные люди могут рефлексивно оценивать свои действия, одобрять те из них, которые соответствуют их ценностям и потребностям, и при этом активно развивать действительность, достойную того, чтобы в ней жить и работать.

Это имеет прямое отношение к информационному поведению сотрудников организации в контексте обеспечения информационной безопасности. Инструктивно-исполнительский характер информационной деятельности сотрудника, чрезмерный контроль со стороны руководства формируют и развивают контролируемую (или безличную) причинную ориентацию сотрудника, что существенно снижает его мотивацию к выполнению правил ИБ и результативность работы.

Автономная ориентация пользователя информационной системы – это фактор влияния на культуру информационной безопасности. Мы обосновали много таких факторов [23], но результат эмпирического исследования с позиций теории самодетерминации показывает, что реципиенты воспринимают автономию как первостепенный фактор [24]. Многочисленные инструкции и правила ИБ, жесткий контроль и наказания за их невыполнение, демонстрирующие недоверие к сотруднику, – все это внешняя мотивация для работника. Культура же связана с внутренними потребностями. Именно с преобладанием внешней контролирующей причинной мотивации, а значит – с низким уровнем культуры ИБ, мы связываем большое число инцидентов угрозы информационной безопасности в организациях по вине сотрудников. В связи с этим работодателям следует стремиться к автономизации сотрудников.

Решение приведенных проблем зависит сегодня не только от работодателя. Цифровизация в глобальном масштабе вызвала серьезные социально-культурные трансформации, которые не могли не оказать влияния на человека как на субъекта информационных отношений. Потребность людей в справедливости, независимости и самостоятельности обострилась и ее реализация принимает все более угрожающие формы, так как ведет к исчезновению традиций законопослушания. Мы разделяем озабоченность А. Лукацкого – ведущего российского эксперта в области информационной безопасности – в том, что свобода как вседозволенность, транслируемая средствами массовой информации последние два десятилетия, негативно сказалась не только на молодежи, но и на всех поколениях. Люди становятся все более непослушными и дерзкими, запреты их раззадоривают, а не пугают или загоняют в рамки. Они не желают соблюдать любые нормы – в жизни, в работе, в том числе правила и инструкции, что приводит к реализации угроз информационной безопасности [25]. Разрушенная система воспитания молодежи, недоверие людей к субъектам власти, невнимание государства к вопросам культуры информационной безопасности, неработающие статьи Уголовного Кодекса – все это обеспечивает перманентный рост числа киберпреступлений и инцидентов угроз информационной безопасности в организациях по вине сотрудников и пока складывается в удручающую картину. Её вряд ли может улучшить внедрение концепции нулевого доверия в информационной безопасности в тех границах, в которых она сейчас разработана техническими специалистами.

Понимание причин осложнившихся проблем – это шаг на пути к их решению. Государству следует, наконец, обратиться к человеку как к пользователю информационных систем, как носителю цифровой культуры, разработать и принять комплексную национальную программу развития культуры информационной (цифровой) безопасности (или кибербезопасности) всех членов общества. К сожалению, разработанный в начале XXI в. проект документа «Основные направления государственной политики в области функцио-

нирования и развития культуры информационной безопасности» так и не был утвержден.

Что касается субъектов экономики, то они могут и должны стать моделью таких информационных отношений, которые основаны на стремлении работодателя к удовлетворению базовых человеческих потребностей работников в автономии в ее лучших традициях, исключающих недоверие, эгоизм и вседозволенность. И модель информационной безопасности, названная 10 лет назад «нулевым доверием», при условии ее совершенствования в обозначенных в настоящей статье направлениях, может стать рычагом изменений в информационно-коммуникационной сфере организации.

Мы разделяем оптимистичные надежды ученых на то, что в будущем будут проведены исследования путей более широкого использования теории социальной детерминации в повседневной практике, стратегическом развитии и социальной политике [26] и в том числе – в сфере информационной безопасности. Это требует междисциплинарных исследований механизмов реализации этой теории в совершенствовании модели нулевого доверия. В технологии ее реализации должны быть изначально заложены принципы гармоничной автономизации пользователей, развития их внутренней ценностной мотивации, расширения вовлеченности в процессы управления ИБ, достижения баланса доверия в информационных коммуникациях работодателя и работника. Полагаем, что не только содержание, но и само название концепции – модель нулевого доверия – нуждается в обновлении. С точки зрения психологии восприятия, сейчас ее название обладает негативной семантической окраской для сотрудников организации, хотя для работодателя – является символом надежности системы ИБ организации. Для гармонизации информационных отношений в организации целесообразно именовать её моделью «сбалансированного доверия».

Субъект реализации этой модели – специалист по защите информации – также нуждается в совершенствовании своих компетенций. Высшее образование способно решить эту задачу. Модель нулевого доверия как объект освоения студентами вуза нуждается в коррекции с точки зрения содержания и форм. Выпускники должны быть способны внедрить эту модель в практику не только на технологическом, но и на пользовательском уровне в любой организации, независимо от формы собственности и отраслевой принадлежности. В процессе обучения требуется и развитие личностной культуры информационной безопасности самих студентов, включая их культуру доверия, автономность и мотивацию к организационной вовлеченности. Только при этом условии они смогут организовать этот процесс на профессиональном уровне.

ВЫВОД

Модель нулевого доверия (*zero trust*), составной частью которой является жестко регламентированное управление доступом пользователей к информационным ресурсам, все шире внедряется в системы информационной безопасности организаций. Однако в настоящее время сложилась тенденция чрезмерного акцентирования внимания работодателя на контролирующей функции управления пользователями и недооценке другой важнейшей управленческой функции – мотивации. Усиленный контроль информационного поведения сотрудников организации, направленный на повышение доверия к безопасности информационных систем, все больше воспринимается ими как недоверие со стороны руководства и вызывает взаимный скептицизм и снижение внутренней мотивации не только к выполнению правил информационной безопасности организации, но и должностных обязанностей в целом.

Снижение доверия работников к работодателю и их мотивации к соблюдению норм информационно-безопасного поведения является следствием не только усиленного контроля, но и негативной глобальной трансформации, выражающейся в нежелании людей следовать установленным нормам и выполнять правила.

Концепция нулевого доверия, положенная в основу системы информационной безопасности организации и интерпретируемая как концепция сбалансированного доверия, способна повысить результативность усилий работодателя по достижению информационно-безопасного поведения сотрудников. Это возможно при условии повышения культуры доверия и автономизации пользователей информационных систем организации как составляющих культуры информационной безопасности. Большой потенциал в решении новых практических задач имеют вузы в процессе подготовки будущих специалистов по защите информации.

СПИСОК ЛИТЕРАТУРЫ

1. InfoWatch. Исследование утечек информации ограниченного доступа в 2020 году. – URL: https://www.infowatch.ru/analytics/analitika/issledovanie-utechek-informatsii-ogranichennogo-dostupa-v-2020-godu (дата обращения: 06.12.2021).
2. SearthInform. Утечки из организаций России. I полугодие. – URL: https://searchinform.ru/blog/2020/08/18/itogi-polugodiya-v-94-sluchaev-iz-organizacij-utekli-poleznye-dlya-moshennikov-dannye/?fbclid=IwAR1tAlLgOePEAY1_FunX219mSKoZdP6xMIur3ElVCAcr4xAr3dCYOuk1YPo (дата обращения: 06.12.2021).
3. SearthInform. Инциденты внутренней безопасности в Российских компаниях. Данные за первое полугодие 2020 года. – URL: https://searchinform.ru/practice-and-analytics (дата обращения: 06.12.2021).
4. Kindervag J. No More Chewy Centers: Introducing the Zero Trust Model of Information Security // Forrester Research. – 2010. – URL: https://www.forrester.com/report/No+More+Chewy+Centers+The+Zero+Trust+Model+Of+Information+Security/-/E-RES56682 (дата обращения: 26.11.2021).
5. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture // National Institute of Standards and Technology. – 2020. – URL: https://csrc.nist.gov/publications/detail/sp/800-207/final (дата обращения: 06.12.2021).
6. Buck C., Olenberger C., Schweizer A., Völter F., Eymann T. Never trust, always verify:

A multivocal literature review on current knowledge and research gaps of zero-trust // Computers & Security. – 2021. – Vol. 110, 102436. – URL: https://www.sciencedirect.com/science/article/ pii/S0167404821002601 https://doi.org/10.1016/j.cose.2021. 102436 (дата обращения: 06.12.2021).
7. Кузнецов С.А. Модель нулевого доверия применительно к корпоративным информационным системам / С.А. Кузнецов, И.А. Куликов, А.А. Фоминых // Актуальные научные исследования в современном мире. – 2021. – № 6-1(74). – С. 59-62.
8. Cittadini L., Spear B., Beyer B., Saltonstall M. BeyondCorp Part III: The Access Proxy. Google; 2016. – URL: https://research.google/pubs/pub45728 (дата обращения: 06.12.2021).
9. Escobedo V.M., Zyzniewski F., Beyer A.E., Saltonstall M. BeyondCorp: The User Experience. Google; 2017. – URL: https://research.google/pubs/pub46366/ (дата обращения: 06.12.2021).
10. Singh J., Refaey A., Shami A. Multilevel security framework for NFV based on software defined perimeter // IEEE Network. – 2020b. – № 34(5). – P. 114–19. DOI: 10.1109/MNET.011.1900563
11. Колпащикова Е.А. Переход от традиционной модели кибербезопасности к модели нулевого доверия / Е.А. Колпащикова, А.А. Юровская // Аллея науки. – 2018. – Т. 4, № 10(26). – С. 942-947.
12. Астахова Л.В. Информационная безопасность: герменевтический подход // Избранные труды Российской школы по проблемам науки и технологий. – Москва: Российская академия наук, 2010. – 186 с.
13. Gigamon. The IT and Security Landscape for 2020 and Beyond and the Role of Zero Trust. Gigamon. – 2020. – URL: https://www. gigamon.com/resources/resource-library/analyst-industry-reports/ar-zerotrust-surveyreport.html (дата обращения: 06.12.2021).
14. American Council for Technology. Zero Trust Cybersecurity: Current Trends. American Council for Technology; 2019. – URL: https://www.actiac.org/zero-trust-cybersecurity- current-trends (дата обращения: 20.11.2021).
15. Астахова Л.В. Онтологический статус доверия в информационной безопасности // Научно-техническая информация. Сер. 1. – 2016. – № 3. – С. 1-9; Astakhova L.V. The ontological status of trust in information security // Scientific and Technical Information Processing. – 2016. – Vol. 43, № 1. – P. 58-65. DOI: 10.3103/S0147688216010123.
16. Astakhova L.V. Developing students' culture of trust as a preventive means of combating cyber extremism // EDULEARN17 Proceedings. – 2017. – P. 4964-4971. – URL: https://library.iated.org/view/ASTAKHOVA2017DEV (дата обращения: 06.12.2021).
17. Астахова Л.В. Проблемы культуры информационной безопасности в условиях цифровой экономики // Научно-техническая информация. Сер. 1. – 2020. – № 2. – С. 28-37; Astakhova L.V. Issues of the Culture of Information Security under the Conditions of the Digital Economy // Scientific and Technical Information Processing. – 2020. – Vol. 47, № 1. – P. 56-64. DOI: 10.3103/S0147688220010062.
18. Deci E.L., Ryan R.M. Intrinsic motivation and self-determination in human behavior. – NY: Plenum Publishing Co, 1985. – 371 p. – URL: https://doi.org/10.1007/978-1-4899-2271-7 (дата обращения: 06.12.2021).
19. CSDT. Center for Self-Determination Theory. – URL: https://selfdeterminationtheory.org (дата обращения: 06.12.2021).
20. Koestner R., Holding A. A generative legacy: SDT's refined understanding of the central role of autonomy in human lives // Motivation Science. – 2021. – № 7(2). – P. 111–112. – URL: https://doi.org/10.1037/mot0000221 (дата обращения: 06.12.2021).
21. Лабзова И.Ю. Теория самоопределения и её применение в зарубежной образовательной практике // Человек и образование. – 2017. – № 3(52). – С. 152-156.
22. Ryan R.M., Deci E.L., Vansteenkiste M., Soenens B. Building a science of motivated persons: Self-determination theory's empirical approach to human experience and the regulation of behavior // Motivation Science. – 2021. – № 7(2). – P. 97-110. – URL: file:///C:/Users/1D1D~1/AppData/Local/ Temp/2021_RyanDeciVansteenkisteSoenens_BuildingAScience_Manuscript.pdf (дата обращения: 06.12.2021).
23. Da Veiga A. Defining organisational information security culture-Perspectives from academia and industry / A. Da Veiga, L. V. Astakhova, A. Botha, M. Herselman // Computers & Security. – 2020. – Vol. 92. – P. 101713. DOI: 10.1016/j.cose.2020.101713 (дата обращения: 06.12.2021).
24. Gangire Y., Da Veiga A., Herselman M. Assessing information security behaviour: a self-determination theory perspective // Information and Computer Security. – Mar 2021. – URL: https://www.emerald.com/insight/content/doi/10.1108/ICS-11-2020-0179/full/html (дата обращения: 06.12.2021).
25. Лукацкий А. Почему не работают политики ИБ, а также наказания за их нарушения?. – URL: https://www.securitylab.ru/blog/personal/Business_without_danger/20720.php (дата обращения: 26.11.2021).
26. Patall E.A. Self-determination theory: Eminent legacy with boundless possibilities for advancement // Motivation Science. – 2021. – №7(2). – P. 117–118. – URL: https://doi.org/10.1037/mot0000223 (дата обращения: 06.12.2021).

Материал поступил в редакцию 07.12.21.

Сведения об авторе

АСТАХОВА Людмила Викторовна – доктор педагогических наук, профессор, профессор кафедры защиты информации Южно-Уральского государственного университета, Челябинск
e-mail: astakhovalv@susu.ru

УДК 004.451:004.415.2.031.43

Ю.Б. Чечиков, В.Е. Секретарев, В.Н. Лукин, А.Л. Дзюбенко, Н.Ф. Алтухова, Л.Н. Чернышов

Методика построения систем управления аппаратно-программными комплексами на основе адаптивной операционной системы реального времени

Рассматриваются проблемы, связанные со снижением затрат времени на сопровождение аппаратно-программных комплексов. Оценивается эффективность замены компонентов операционной системы при традиционном и объектно-ориентированном подходе. Предлагается вариант Адаптивной операционной системы реального времени (ОС РВ) для быстрого подключения бортовой аппаратуры, который позволяет существенно снижать сроки разработки серийных и индивидуальных изделий и повышать их надёжность.

Ключевые слова: *аппаратно-программный комплекс, методика, объектно-ориентированное программирование, адаптивность системы, аппаратный интерфейс передачи данных, полиморфизм*

DOI: 10.36535/0548-0019-2022-03-3

ВВЕДЕНИЕ

Построение любой системы основано на обмене информацией как между её частями, так и с другими системами. Своевременная и достоверная информация – это то, без чего невозможно оценить состояние объекта, выработать адекватные управляющие решения.

Если между отдельными частями системы есть связи, то можно контролировать функционирование частей и управлять ими. При больших потоках первичных данных в системах реального времени скорость и надежность передачи информации в значительной степени определяют качество управления объектом.

Возникают вопросы: как создать методику разработки аппаратно-программного комплекса, чтобы сделать систему обмена и передачи данных быстрее и надежнее, чем при традиционных подходах? Какие средства надо применять, чтобы продлить жизненный цикл систем, повысить их надежность и живучесть в процессе эксплуатации?

Необходимы средства и решения, позволяющие правильно и эффективно организовать систему обмена информацией между всеми уровнями иерархии. На основе этих средств, в дальнейшем, можно строить обширную и развитую систему обработки информации, систему управления и далее. Качество методов внедрения и стоимость сопровождения системы сбора информации и управления во многом определяют успешность её функционирования, дальнейшего развития и масштабирования.

Критерием адаптивности системы к изменениям будем считать время, стоимость и трудоемкость внесения изменений в программное обеспечение, что, в конечном счете, определяет длительность ее жизненного цикла. Считается, что затраты на исправление обнаруженных ошибок и дальнейшее развитие комплекса могут составлять до половины стоимости его на протяжении жизненного цикла [1].

Рассмотрим проблемы построения системы в том случае, когда в ее состав нужно добавить новое устройство, например микроконтроллер.

АНАЛИЗ ПРОБЛЕМЫ СОПРОВОЖДЕНИЯ И МОДИФИКАЦИИ ПРОГРАММНЫХ КОМПЛЕКСОВ

При подключении новых устройств в процессе сопровождения и эксплуатации аппаратно-программных комплексов возникают проблемы внешнего и внутреннего характера. Их нужно учитывать при разработке методики построения систем.

Внешние проблемы сопровождения носят объективный характер. Для подключения нового устройства программист должен разобраться в новой логике устройства, написать внутренние программы для микроконтроллера, согласовать обновленную логику его работы с правилами работы в системе.

Для программирования микроконтроллеров программист использует специализированные интегрированные среды разработки (*Integrated Development Environment – IDE*), поставляемые фирмами – разработчиками устройств, например, *CubeMX, Keil µVision*.

Если новый микроконтроллер будет той же фирмы, что и старый, то, с большой вероятностью, инструментальные средства разработки программ останутся прежними. Если же микроконтроллер будет другой фирмы, то придётся переходить на новую среду разработки, разбираться в ней, осваивать ее и быть готовым к большому количеству подводных камней.

Чтобы разобраться в новой документации и среде разработки, квалификация прикладного инженера должна быть не ниже, чем у разработчика среды, и для достижения необходимого уровня подготовки, можно потратить несколько лет. Много сил уходит и на настройку среды: нужно понять, где и какую галочку поставить, чтобы все заработало так, как надо. Подобная работа выполняется один раз и, естественно, запомнить все настройки невозможно.

Казалось бы, можно воспользоваться автоматической генерацией программного кода (*IDE*). Но в этом случае текст получается тяжелый для восприятия: непонятна структура программы и связь её частей, неясно назначение функций и переменных. В результате быстро внести изменения в программу не представляется возможным, так как, поменяв хотя бы одну функцию или переменную, нельзя точно предсказать, какая реакция на эти изменения будет у программы. Если изменения в программе сделаны с ошибкой, то это может породить массу других ошибок, совершенно не предсказуемых и внешне не связанных друг с другом.

Как следствие, программисты начинают бояться вносить изменения в программу и отказывают клиентам в ее модификации. Поэтому, если один раз задача была решена успешно, то программный код уже не модифицируется, и система доживает свой срок без изменений.

Внутренние проблемы сопровождения носят субъективный характер и, во многом, определяются квалификацией разработчиков [2].

Вопросами удобства сопровождения следует заниматься на этапе проектирования системы – при выборе ее архитектуры, инструментальных программных средств, внутренних стандартов программирования в коллективе.

Разработчик должен заранее запланировать возможное развитие системы, обеспечить легкость поиска и исправления ошибок, иначе, после сдачи её в эксплуатацию, необходимость развивать систему, масштабировать её станет "приятной" неожиданностью для сопровождающего программиста. В результате некачественного проектирования может выясниться, что архитектура системы оказалась необоснованно сложна, связи между ее частями слишком запутаны и неочевидны, и, поэтому, быстро внести требуемые изменения, практически, невозможно. Как уже упоминалось выше, квалификация сопровождающего программиста должна быть выше квалификации разработчика, поскольку изменения надо вносить в уже работающий комплекс в короткие сроки [3].

Поэтому при разработке новой системы надо стремиться не к тому, чтобы сдать ее как можно быстрее, а к тому, чтобы обеспечить ее удобное сопровождение на протяжении всего жизненного цикла. И для любой предметной области этот подход следует рассматривать как фундаментальный принцип проектирования.

Удобство сопровождения может обеспечить технология программирования, которая обычно не используется для разработки аппаратно-программных комплексов, а именно – объектно-ориентированный подход (ООП) с его понятиями интерфейсов, абстрактных базовых классов, вертикального и веерного наследования (один предок и несколько прямых потомков), полиморфизма.

Каждый аппаратный интерфейс передачи данных (*UART, SPI, USB*; *MIL-STD1553B*) имеет свою логику работы, но, с точки зрения ООП, все эти интерфейсы могут быть приведены к одному ООП-интерфейсу или абстрактному базовому классу, в котором объявлены только переменные и функции приема и передачи. Конкретная реализация функций при веерном наследовании будет своя для различных потомков одного уровня. За счет наследования обеспечивается единый подход к алгоритмам работы, к стандартизации имен переменных и функций всех родственных объектов иерархии. Поэтому надежность и понимание программы значительно улучшаются, а стоимость сопровождения снижается.

Использование полиморфизма и виртуальных функций облегчает добавление нового устройства в систему. Для этого в иерархию классов добавляется потомок, в котором реализованы методы, отражающие только особенности нового устройства, а общее для всех устройств поведение не дублируется, а берется у предков. Конкретные особенности поведения каждого устройства обеспечивают различные реализации при едином интерфейсе, что и составляет суть полиморфизма. Система получается открытой, удобной к расширению и масштабированию.

Таким образом, использование технологий ООП обеспечивает одновременное функционирование существующих и вновь появившихся в системе устройств без переписывания её заново.

Рассмотрим проекты с малой детализацией, например, системы сбора аналоговой информации на микроконтроллерах 1986VE4Y, 1967VK01T, TMS320F28335. Решаемые задачи, в принципе, одинаковы, функционал близок по смыслу, но для каждого микроконтроллера он свой, и программисту приходится держать в голове три версии программного кода. Хотя, по сути, надо принять данные с аналого-цифрового преобразователя (АЦП), оцифровать их, отправить внешней задаче и синхронизировать доступ к этим данным. Алгоритм всюду один. Различия находятся только в настройках регистров аналого-цифрового преобразователя для каждого микроконтроллера. Логичным решением будет создать базовую иерархию, на которой реализованы общие задачи (прием/оцифровка/передача), а в нижний уровень иерархии поместить конкретную работу с АЦП для каждого микроконтроллера.

Следующий уровень иерархии – это, например, комплексная система управления (КСУ), которая комплектуется с блоком датчиков, вычислительной частью и исполнительными механизмами. КСУ должна получить первичную аналоговую информацию, но уже оцифрованную (прием данных), эти данные обраба-

тываются в соответствии с законами управления и передаются исполнительным устройствам. Опять получается общая схема: прием/обработка/передача.

И, наконец, большие системы: целиком собранный борт самолета. На этапе финального комплексирования собираются вместе приборы и комплексы от разных заводов и институтов, подготовленные программистами с разными подходами. У каждого разработчика все работает по отдельности, но, когда все ставится на комплекс, что-то отказывает. Разобраться, у кого что не работает, крайне сложно и затратно по времени. Основные проблемы создают механизмы приема и передачи информации между устройствами. Внести оперативно исправления в программное обеспечение, реализованное в парадигме процедурно-ориентированного программирования, очень трудно.

Системы, разработанные в методике ООП, изначально ориентированы на изменения. Для того, чтобы как-то стандартизовать разработку высокоуровневой иерархической системы, необходимо иметь единый фундамент [4, 5]. Во всех системах данные нужно собрать, обработать и передать. На уровне базового класса все едино, но конкретная реализация низших уровней иерархии будет иметь свою конкретику – вычисления, интерфейсы ввода/вывода данных, исполнительные механизмы. Разработанная нами Адаптивная операционная система реального времени (ОС РВ) инвариантна к различиям и имеет базовый уровень реализации в виде автономной адаптивной системы ввода/вывода. Она работает с объектами верхнего уровня иерархии, реализующими прием/запись/передачу данных, а для конкретного устройства функционал вызывается с нижнего уровня за счет механизма виртуальных функций и динамического полиморфизма.

Получается единый подход, единая структура алгоритмов и данных. Предложенное нами решение подходит под все многообразие задач управления и программирования аппаратно-программных комплексов.

В парадигме процедурно-ориентированного программирования для каждого микроконтроллера создаются свои библиотеки функций, пусть сильно совпадающие, но имеющие в основе вызовов обращения к конкретному функционалу. Выделить в отдельную библиотеку общую часть не представляется возможным. С увеличением количества микроконтроллеров значительно растет объем программного кода, который надо помнить и хорошо в нем разбираться. Для программиста это очень трудоемкая задача, которая существенно удорожает разработку.

РЕШЕНИЕ РАССМАТРИВАЕМОЙ ПРОБЛЕМЫ

Выход видится один – работать в парадигме объектно-ориентированного программирования. Например, для работы с *SPI* (*Serial Peripheral Interface*) нужно создать базовый класс для *SPI*. Ему все равно, какой используется вычислитель. Этот базовый класс копируется в те места, где требуется работа с *SPI*: различные микроконтроллеры, ядра микропроцессоров, но без конкретики. Конкретная настройка режимов работы (*Master* или *Slave*) реализуется в классах нижнего уровня. Все *SPI* имеют в базовом классе виртуальные функции инициализации (Init()), чтения *FIFO* (*ReadFIFO*()) и записи в *FIFO* (*WriteFIFO*()), которые реализуются в потомках. Вызов конкретной функции выполняется динамически из базового класса в процессе работы. Таким образом, при единой структуре появляется видовое многообразие частных аппаратно-программных решений, внедрение которых поддерживается соответствующей документацией.

Аналогично в других предметных областях. Например, в медицине при автоматизации биохимических лабораторий следует учитывать парк автоанализаторов, методы сбора и обработки поступающей информации. Даже проведение одного и того же исследования в разных лабораториях различно и определяется наличием соответствующих химических реактивов и измерительных приборов. Объединение нескольких биохимических лабораторий потребует внутренних стандартов на их разработку, потому что нужна единая структура, единый формат обмена информацией между производственными участками лаборатории и самими лабораториями. Снизить трудоемкость комплексной разработки в рамках процедурного подхода весьма затруднительно. В отсутствие единого фундамента для разработки при добавлении новой лаборатории программный код значительно разрастается.

Если рассмотреть ситуацию с позиций ООП, то можно выделить единый сценарий работы: получить список заказов для проведения того или иного исследования, организовать очередь в автоанализаторе и получить результаты измерений, сформировать итоговый бланк-ответ, который отсылается лечащему врачу. Имея общий для всех лабораторий базовый класс, можно резко удешевить разработку, упростить управление и повысить технологичность сопровождения.

Иерархия систем, реализованных в парадигме ООП, инвариантна к предметной области. Программного кода меньше, структура единая, сопровождать легче, длительность жизненного цикла системы увеличивается.

АДАПТИВНАЯ ОПЕРАЦИОННАЯ СИСТЕМА РЕАЛЬНОГО ВРЕМЕНИ

С учетом изложенных соображений, нами была разработана Адаптивная ОС РВ, которая позволяет создавать оптические и цифровые бортовые вычислительные системы, системы организации беспроводной передачи данных (по радиоканалам, Wi-Fi, GPS, Bluetooth, лазерной передачи данных), обладающие свойствами быстрой адаптации к конкретным условиям и удобством эксплуатации на протяжении жизненного цикла, а также снижающие сроки и трудоемкость разработки серийных и индивидуальных изделий.

Адаптивность системы состоит в том, что это не универсальное средство, подходящее под все задачи, а средство, специализированное под конкретный класс задач с последующей адаптацией под особенности решаемой задачи. Универсальные средства очень тяжеловесны и негибки в силу своей универсальности. В результате, большая часть возможностей, которые не нужны для решения конкретной задачи, попросту не используется.

В Адаптивной ОС РВ нет состояния блокированной задачи, что позволяет не подвешивать ресурсы на ожидание завершения других задач. В случае отсутствия блокировок ресурсы центрального процессора и аппаратной части используются максимально полно, поэтому на менее производительных процессорах, с точки зрения других операционных систем, можно решать те же задачи.

В состоянии блокированной задачи следует передавать управление другим вычислительным ресурсам, а в случае, если несколько задач блокируется, то нужно иметь еще больше дополнительных вычислительных ресурсов.

Отсутствие блокировок позволяет выстраивать коммуникации между частями системы без задержек – данные приходят и сразу же обрабатываются, не внося дополнительные фазовые задержки.

Важная особенность ОС РВ – это система обработки прерываний. Обработчик прерываний работает настолько быстро, что даже вложенные прерывания не создают проблем для работы ядра ОС РВ и передачи данных.

Для инженера открыт доступ к аппаратной части – операционная система его никак не блокирует и не ограничивает, она позволяет подключать большое количество устройств по различным интерфейсам. Для высокоскоростной передачи данных можно использовать оптоволокно.

Ядром операционной системы реального времени является Автономная адаптивная самосинхронизирующаяся система ввода/вывода (ААССВВ).

Автономность. ААССВВ локализована в виде отдельного программного комплекса и не связана с внешней операционной системой, которая может использоваться на данном *MCU* (*Multi Controller Unit* – микроконтроллер) или *CPU* (*Central Process Unit* – центральный процессор). Это обеспечивает возможность её переноса с одной аппаратно-программной платформы на другую; может потребовать некоторых усилий, но не является многолетней разработкой.

Адаптивность. При смене микроконтроллера следует только перекомпилировать программный код под ядро микроконтроллера.

В случае эволюционной смены программной или аппаратной базы, когда производители постепенно переходят на новые программно-аппаратные решения, предложенная нами система адаптируется к изменению внешних условий без серьезных доработок. Это обеспечивает длительность ее функционирования в составе комплекса и значительно увеличивает его жизненный цикл. Система не отмирает при изменении условий внешней среды, а адаптируется к ним.

Самосинхронизация. Есть общая часть памяти, к которой имеют доступ аппаратная и программная части одновременно. ААССВВ автоматически синхронизирует доступ к общей памяти, чтобы не было конфликтов между программной и аппаратной частями. Синхронизация доступа внешней программы и контроллера осуществляется при чтении/записи общей памяти.

Система ввода/вывода. ААССВВ обеспечивает двунаправленность потоков данных между устройствами и внешней средой. Система ввода/вывода создает условия для работы с подключенными периферийными устройствами ввода/вывода, состоящими из ЦАП, АЦП, SPI, UART, МКIO, Ethernet, а также для диспетчеризации потоков данных между устройствами. Диспетчеризация состоит в том, чтобы определять абонентов – кому доставить информацию и от кого её получить.

После создания ААССВВ происходит привязка ее к аппаратной части – специализация под конкретные условия работы – тип ядра микропроцессора и микроконтроллера.

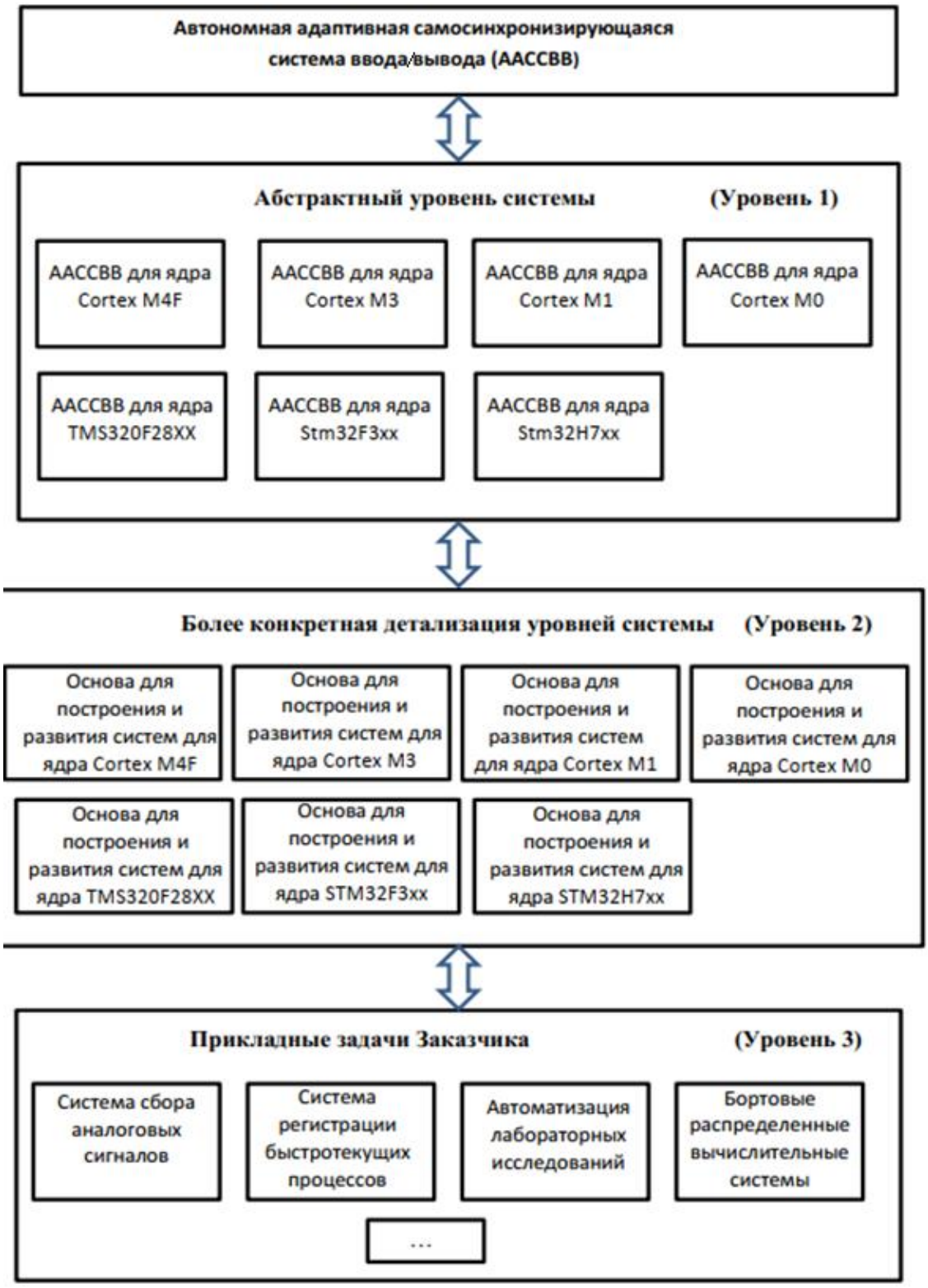
Абстрактный уровень ААССВВ (Уровень 1 на рисунке) обобщает свойства систем, построенных на конкретном ядре, например, *Cortex M4F*, *Cortex M3*, *Cortex M1*. На этом уровне содержатся абстрактные базовые классы, в которых частично реализованы алгоритмы обмена данными между устройствами по разным интерфейсам. Задача уровня – обеспечить единую структуру и предложить наиболее универсальное решение для построения систем в рамках **одного ядра**. ААССВВ обеспечивает наиболее легкий перенос программ с одного ядра на другое. Здесь не учитываются физические характеристики аппаратной части.

Более конкретная детализация подразумевает наследование от базового класса, а механизм наследования и виртуальных функций (Уровень 2 на рисунке) позволяет создавать систему, которая будет дорабатываться и уточняться в конкретной реализации. За счет полиморфизма облегчается добавление нового устройства в систему. В этом случае в иерархию классов добавляется потомок, в котором реализованы методы, отражающие только особенности нового устройства, а общее для всех устройств поведение **не дублируется** и берется у предков.

Конкретные особенности поведения каждого устройства, настройка регистров интерфейсов, обеспечивают различные реализации при едином базовом классе, что и составляет суть полиморфизма в объектно-ориентированном программировании. Система получается открытой, удобной к расширению и масштабированию и обновлению документации для пользователей.

Использование иерархии классов Уровня 2 при разработке системы позволяет на ранних стадиях проектирования учитывать взаимосвязи различных этапов обработки данных (АЦП, МКИО, UART, SPI).

К моменту выхода на прикладные задачи все коммуникации должны быть реализованы. Подключение нового устройства (Уровень 3 на рисунке) – это создание очередного потомка с конкретной физической реализацией. На этом уровне за счет веерного наследования от абстрактных базовых классов обеспечивается видовое многообразие частных решений построения вычислительных систем, что позволяет прикладному программисту с небольшими затратами добавить новое устройство и сосредоточиться на **своих** задачах.



Создание систем с использованием Адаптивной операционной системы реального времени

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

Полученные нами результаты показали, что общий код программы можно переносить с одного ядра на ядро другого производителя. В систему заложено свойство адаптации и инвариантности к существующей и вновь создаваемой аппаратной части. В рамках представленного подхода разработана Адаптивная операционная система реального времени с автономной системой ввода/вывода, которая является основой для построения систем управления и сбора информации различных уровней сложности, и методика её внедрения.

Существенный выигрыш такого решения – снижение стартовых затрат на разработку новых систем, а главное – возможность существенного продления жизненного цикла этих систем при модификации бортового оборудования. Как показывает опыт, при переходе от процедурного программирования к объектно-ориентированному объем программного кода гарантированно сокращается как минимум в 2 раза, а повышение читабельности текста переходит на другой качественный уровень.

За счет видового многообразия состав и сложность вычислительной системы можно комбинировать.

ЗАКЛЮЧЕНИЕ

Для создания систем различных уровней сложности предложен подход и средства к построению фундамента, на основе которого можно разрабатывать прикладные системы со своим функционалом. Таким образом, разработчик стартует **не с нуля**, а с уровня, обеспечивающего гарантированный бесперебойный обмен информацией между устройствами различных типов.

В ходе разработки [6] был создан прототип системы, настроенный на работу не с отдельным микроконтроллером, а с семейством микроконтроллеров и центральных процессоров, основанных на конкретном ядре (Cotrex M4F, Cotrex M3, Stm32H7xx b и т. д.). В результате, при построении системы на основе созданного прототипа, снижаются требования к квалификации разработчика и сопровождающего программиста, которые могут использовать в своей работе соответствующие методические руководства. Таким образом обеспечено повышение технологичности сопровождения аппаратно-программных комплексов. Основное внимание в разработке было уделено надежности программного обеспечения, повышению скорости внесения изменений и снижению стоимости этого процесса, многократному использованию имеющихся наработок (за счет иерархии классов объектно-ориентированного программирования). В этом случае появляется преемственность разработок и повышается надежность всего семейства изделий.

На основе единой иерархии классов становятся возможными решения, которые учитывают специфику области функционирования будущих систем и обеспечивают видовое многообразие аппаратно-программных решений соединения с оборудованием или частями системы. Использование Адаптивной операционной системы реального времени снижает сроки и трудоемкость разработки серийных и индивидуальных изделий. Область применения Адаптивной ОС РВ инвариантна к предметным областям: промышленность, оборона, медицина, образование, коммуникационные сервисы, что все более актуально сегодня.

Вечное сопровождение – это естественное состояние программного обеспечения и предлагаемая операционная система облегчает этот процесс. Сопровождение может идти по пути углубленной специализации отдельных систем, либо по пути интеграции существующих аппаратно-программных комплексов.

СПИСОК ЛИТЕРАТУРЫ

1. Глаас Р., Нуазо Р. Сопровождение программного обеспечения: пер. с англ. – Москва: Мир, 1983. – 156 с.
2. Lukin V.N., Dzyubenko A.L., Chechikov Yu.B. Approaches to User Interface Development // Programming and Computer Software. – 2020. – Vol. 46, № 5. – P. 316-324.
3. Емелин И.В., Лукин В. Н., Эльчиян Р.А. О жизненном цикле системы реального времени // Прикладная информатика. – 1985. – № 2. – С. 135–143.
4. Вигерс К., Битти Д. Разработка требований к программному обеспечению. 3-е изд., дополненное / пер. с англ. – Москва: Изд-во «Русская редакция»; Санкт-Петербург: БХВ-Петербург, 2020. – 736 с.
5. ГОСТ Р ИСО/МЭК 14764–2002. Информационная технология. Сопровождение программных средств. – 2002. – URL: https://docs.cntd.ru/document/ 1200030195.
6. Чечиков Ю.Б. Основа для построения систем обмена данными / Ю.Б. Чечиков, В.Е. Секретарев, В.Н Лукин, А.Л. Дзюбенко, Н.Ф. Алтухова, Л.Н. Чернышев // Научно-техническая информация. Сер. 2. – 2022. – № 2. – С. 25-28.

Материал поступил в редакцию 30.01.22.

Сведения об авторах

ЧЕЧИКОВ Юрий Борисович – кандидат физико-математических наук, доцент, Московский авиационный институт
e-mail: yourych@mail.ru

СЕКРЕТАРЕВ Виталий Евгеньевич – специалист в области систем обработки информации и управления, инженер, Московский авиационный институт
e-mail: sinoptik.mnpk@gmail

ЛУКИН Владимир Николаевич – кандидат физико-математических наук, профессор Московского авиационного института
e-mail: lukinvn@list.ru

ДЗЮБЕНКО Алла Леонидовна – кандидат технических наук, доцент, кафедра «Бизнес-информатика» Финансового университета при правительстве РФ, Москва
e-mail: al_dz@list.ru

АЛТУХОВА Наталья Фаридовна – кандидат экономических наук, доцент, Финансовый университет при правительстве РФ, Москва
e-mail: nfaltuhova@fa.ru

ЧЕРНЫШОВ Лев Николаевич – кандидат физико-математических наук, Финансовый университет при правительстве РФ, доцент, Московский авиационный институт
e-mail: levchern@gmail.com

ДОКУМЕНТАЛЬНЫЕ ИСТОЧНИКИ ИНФОРМАЦИИ

УДК 004.738.5:001.811

Н.Г. Иншакова, И.А. Панкеев

Нарушение норм использования интернет-ресурсов: о плагиате и ошибках цитирования

На примере образовательной среды показано, как за годы пандемии изменилось отношение к нормам использования интернет-ресурсов. Рассмотрены базовые понятия, характеризующие заимствование информации, названы причины некорректного обращения с чужими произведениями. Определены смысловые погрешности цитирования, типичные нарушения правил оформления заимствованного текста. Предложен вариант систематизации основных ошибок цитирования.

Ключевые слова: *сетевая коммуникация, интернет, контент, информация, заимствование, плагиат, ошибки цитирования*

DOI: 10.36535/0548-0019-2022-03-4

ВВЕДЕНИЕ

Первый из четырех законов экологии американского биолога Барри Коммонера «все связано со всем» – применим и к современной информационной сфере [1]. Медиаповедение в 2022 г. значительно отличается от медиаповедения трехлетней давности. В течение последних лет не только бытовое, но и профессиональное общение почти полностью перешло в дистанционный формат: от обсуждения производственных вопросов до – что важно в контексте предлагаемого исследования – обмена оперативной информацией, сведениями о публикациях, данными, почерпнутыми из разных источников. Если и до пандемии поиск информации в каталогах библиотек и работа с литературой в библиотеке воспринимались едва ли не как анахронизм, то в сегодняшней ситуации обращение исключительно к сетевому контенту оценивается как данность. Даже при проведении научных исследований, предполагающих изучение большого количества работ и создание основательной источниковедческой базы.

Нематериальность чужого произведения в сочетании с легкостью доступа к информации, повсеместное использование ее с самыми разными целями сформировали новый тип медиапотребителя. Современные пользователи стали воспринимать сетевые ресурсы как нечто, принадлежащее всем и созданное для бесконтрольного применения. В результате резко трансформировалось отношение к таким базовым ценностям, как этика, право, уважение к результатам чужого труда.

Особенно остро эти проблемы стоят в образовательной среде. Молодые люди, с детских лет владеющие компьютерной грамотностью, не обладают должной информационной культурой, одним из безусловных показателей которой является знание этических норм работы с информацией. Образовательные учреждения принимают в свою среду «информационно инфантильных» учащихся и выпускают их в таком же статусе, нанося ущерб *будущему обществу*. Поэтому именно в системе высшего образования важно изучать различные стороны этой непростой ситуации и искать пути формирования этичного отношения к информации и ее использованию.

Проблема присваивания чужих произведений (от откровенного плагиата до неправомерного цитирования) рассматривается в многочисленных научных публикациях. Исследователи приходят к выводу, что «в России так же, как в США и странах Европы, образовательный ресурс не избежал студенческого увлечения заимствованием готовых академических работ», и считают, что «принятие дополнительных организационных мер в учебных заведениях в совокупности с включением инновационных решений контроля образовательного процесса позволит сократить количество нарушений академической этики и, следовательно, противодействовать проявлениям недобросовестности, сказывающимся на уровне подготовки специалистов» [2]. Всё чаще поднимается вопрос о необходимости

создания механизмов противодействия некорректному заимствованию, поскольку их отсутствие наносит существенный урон высшему образованию и науке [3]. Внимание представителей высшей школы привлекают участившиеся случаи нарушений академической этики в научных публикациях и квалификационных работах (от курсовых и дипломных до диссертаций) в условиях бурного развития информационно-коммуникационных технологий [4].

Высказывается предположение, что «распространение академического плагиата является симптомом несоответствия между действующими в образовании традициями и тенденциями постмодерна» [5].

Оценивая недобросовестность не только студентов, но и преподавателей и опираясь на результаты социологических исследований и примеры борьбы с академической недобросовестностью в вузах России и стран Запада, автор одной из публикаций видит возможность искоренения некорректных заимствований в «максимизации образовательных и научных процессов» [6].

В меньшей мере, чем плагиат, в научных публикациях представлена такая тесно связанная с явлениями заимствования и особенно актуальная сейчас тема, как цитирование. Правовые и этические аспекты цитирования уже обсуждались в ряде наших статей [7–10].

Цель настоящей статьи рассмотреть, как за годы пандемии изменилось отношение к нормам и правилам использования информации, прежде всего той, что размещена в Интернете. А именно сетевые публикации стали как никогда востребованными и используются чаще всего. Отметим и такое, влияющее на ситуацию в целом обстоятельство: обращение к бумажным источникам, выложенным в сети, сопровождается многочисленными ошибками при оформлении ссылок (нарушений требований библиографического описания стало еще больше после введения нового национального стандарта [11]), что вольно или невольно приводит к расширению границ некорректного использования чужих произведений.

Нами предпринята попытка проанализировать и систематизировать наиболее распространенные случаи этичного (цитирование) и неэтичного (плагиат) использования интернет-контента в работах молодых исследователей, к которым кроме студентов старших курсов гуманитарных вузов мы относим магистрантов и аспирантов. Как одна из форм заимствования объектом дальнейшего детального исследования может стать рерайт.

В настоящей работе применялись общелогические методы анализа, синтеза, сопоставления и обобщения, а также метод включенного наблюдения – прочитано более 500 работ: научные квалификационные, выпускные квалификационные, курсовые, контрольные, письменные ответы на вопросы по изучаемым темам. Использовался также метод онлайн-опроса (более одной тысячи письменных ответов).

Данные, полученные в результате изучения публикаций и путем «полевых» методов сбора информации, побудили нас обратиться к понятийному аспекту проблем заимствования. Без этого группировка случаев некорректного использования не могла быть в полной мере логически обоснованной.

О СОДЕРЖАНИИ ПОНЯТИЙ, СВЯЗАННЫХ С ИСПОЛЬЗОВАНИЕМ КОНТЕНТА

В различных ситуациях использования чужого контента наиболее распространенными являются понятия «заимствование» и «плагиат», которые повсеместно рассматриваются как синонимы.

С нашей точки зрения, ключевым (и даже родовым, как будет показано далее) следует считать понятие **«заимствование»**, значение которого необходимо уточнить, поскольку в публикациях о нарушении академической этики довольно часто игнорируется полисемия этого слова. Итак, «заимствование» в большинстве словарей нормативной лексики трактуется следующим образом: «1. Заимствовать. З. сюжета. З. идей. З. слов. З. темы. 2. То, что перенято, взято, почерпнуто откуда-л. Иноязычные заимствования» [12]. В лингвистике заимствование – это процесс усвоения в одном языке слова, выражения или его значения из другого языка, а также результат этого процесса – само заимствованное слово, т.е. в языковом отношении заимствование трактуется как позитивное естественное явление лексической диффузии, а значит исследователям проблем плагиата не стоит игнорировать факт существования этого слова не только в негативном смысле.

Мы будем употреблять словоформу «заимствование» не в лингвистическом, а в нормативном значении, для которого в словарях синонимов предлагаются следующие варианты: *повторение* **(**самый частотный**),** *подражание, усвоение, компиляция, плагиат.*

Понятие **«плагиат»** (от лат. *plagio* – похищаю) в наиболее авторитетных словарях нормативной лексики, в энциклопедических и справочных изданиях дано в одном значении: «умышленное присвоение авторства на чужое произведение литературы, науки, искусства, изобретение или рационализаторское предложение (полностью или частично)» [13]. Важным для понимания сути дальнейших рассуждений является эпитет «умышленное» и уточнение: «Плагиат выражается в публикации под своим именем чужого произведения, а также в заимствовании фрагментов чужих произведений без указания источника заимствования» [14].

В синонимическом ряду понятие «плагиат» представлено словами: *повторение, подражание, присвоение, контрафакция, литературное воровство, заимствование.* Однако, как уже было отмечено во Введении, за последние три года в информационном обществе произошли значительные изменения медиаповедения, прежде всего по отношению к использованию информации. Одним из последствий размывания этических норм стало толерантное восприятие самого явления «плагиат», что нашло отражение и в его актуальной трактовке: «Понятие плагиата не имеет вполне определённого содержания, и в частных случаях не всегда возможно однозначно отделить его от сопредельных понятий: подражания, заимствования, соавторства и других подобных случаев сходства произведений» [15]. В спорном по сути, в этом определении к тому же абсолютно неверно приводятся «сопредельные» понятия (соавторство ни в коей мере не причисляется к плагиату), что под-

утверждает целесообразность нашей попытки внести ясность в терминологию.

Дальнейшее изучение источников по рассматриваемой нами проблеме подтвердило явную тенденцию к изменению семантики слова «плагиат» и сути обозначаемого им действия. Наши выводы были не вполне ожидаемы. Оказалось, что, если ранее понятие «плагиат» действительно означало только негативное и, главное, абсолютно однозначно трактуемое явление, то теперь и сам термин, и объект дефиниции не столь конкретны, а отношение к последнему терпимое и даже снисходительное. Как ни парадоксально, но именно в образовательной среде. Появилось мнение: если студент списывает работу, то это свидетельствует о несамостоятельности, незрелости его мышления, а не о плагиате [17]. Более того, предложено различать высокий плагиат (в науке, искусстве) и бытовой, т. е. присвоение результатов интеллектуального труда во всех других сферах [17].

Если преподаватели снисходительны к плагиату, то вполне естественно, что студенты лояльны в еще большей степени. Так, в результате изучения психологических предпосылок студенческого плагиата (авторы публикации [16] опросили 75 человек) было обнаружено, что студенты, «несмотря на понимание значения слова «плагиат», рассматривают многие ситуации плагиата как допустимые», в частности, они считают компилирование и использование чужого текста под своим именем нормальным явлением. При этом «более склонные к использованию плагиата студенты отличаются более низким уровнем самоинтереса, уверенности и коммуникативных мотивов» [16].

Те же результаты были получены при проведении онлайн-опроса, о котором мы писали в начале настоящей статьи. Студентам и магистрантам гуманитарных факультетов было предложено ответить на вопрос: «Является ли использование чужого текста без ссылки на автора и источник: 1) правовым нарушением; 2) этическим нарушением; 3) не является нарушением». Понятие «текст» предлагалось трактовать в широком значении (вербальный, визуальный и их сочетание – креолизованный), так как важно было выявить отношение к заимствованию любого контента. Треть опрошенных отметили, что не считают заимствование чужого текста нарушением правовых и этических норм на том основании, что текст размещен в социальных сетях и потому может использоваться всеми. (Показательно, что в значительной части рассматриваемых текстов присутствовали те или иные виды заимствований.) Половина учащихся мотивировали допустимость использования чужого текста тем, что он находится в открытом доступе; автор исходного текста не указан; содержание текста было пересказано. Такая позиция свидетельствует не только о незнании правил обращения с интернет-контентом, но и о девиации медиаповедения, что связано с непониманием этических норм и самой сути интеллектуальной собственности. Симптоматично, что при этом 70% опрошенных категорически против того, чтобы их собственные работы использовались без их согласия и без указания их авторства.

ХАРАКТЕРИСТИКА ОСНОВНЫХ ВИДОВ ЗАИМСТВОВАНИЙ ТЕКСТОВ

Для того чтобы разобраться в нюансах действий, связанных с использованием источников информации, мы предлагаем зафиксировать понятие «заимствование» (в значении «то, что перенято, взято, почерпнуто») в качестве **родового**. На первом уровне этой классификации (речь пойдет о вербальном контенте) – заимствования этичные и неэтичные (рис. 1). В качестве основания деления нами выбрана этика поведения. Как мы уже отмечали, не любое заимствование маркируется как негативное, а по отношению к манипуляциям с контентом является неэтичным. Однако непременное условие этичного заимствования – это указание автора и источника. Показательно, что этот признак (ссылка на источник) присутствует во всех определениях плагиата, а значит, с его помощью абсолютно все действия, связанные с использованием информации, можно четко разделить на два вида: если есть ссылка на оригинальную работу, то информация не украдена; если ссылки нет – работа присвоена. В абсолютной «прозрачности» такого деления можно не сомневаться, даже предполагая, что существуют некие исключения из правила. Данного параметра достаточно, чтобы понять, с явлением какого рода мы имеем дело: с цитированием или плагиатом. Таким образом, этика как один из важных регуляторов социального поведения личности хорошо ориентирует и в этом частном случае. Причем, по нашему мнению, она не нуждается в дополнительных эпитетах (научная, академическая, студенческая этика).

На основе изучения учебных работ, базирующегося на методе включенного наблюдения, нами был сделан вывод о возможности деления явлений первого уровня (цитирование – плагиат) классификации по признаку осознанности совершаемых действий. Таким образом, в плагиате было выделено два подвида: умышленный и «наивный». Возможен вопрос о правомерности этих эпитетов, но они вполне семантически оправданны по отношению к предлагаемому признаку. Умышленным (т. е. преднамеренным, сознательным и даже «злостным, нарочитым и демонстративным» [18]) принято считать любое присвоение результатов чужой интеллектуальной деятельности, однако в образовательной среде довольно часто такое присвоение происходит из-за инфантильности отдельных представителей студенческого сообщества, из-за отсутствия навыков исследовательской работы, непонимания исключительности результатов чужого труда. Это означает, что действия, которые привели к плагиату, обозначенному нами как «наивный», можно признать неумышленными. Почему именно эта лексема представляется уместной, становится понятно при характеристике её разновидностей, которые продолжают классификационный ряд заимствований уже на следующем уровне. «Наивный» плагиат первого типа (см. рис. 1) появляется в тех случаях, когда учащийся, а нередко и исследователь, в процессе изучения литературы даже не задумывается о необходимости фиксировать понравившиеся ему отдельные мысли, выражения, фразы, не знает о требовании указывать в каждом конкретном случае источник

Рис. 1. Виды заимствований текстов

(повторим – это сущностный признак плагиата), страницу и прочие данные идентификации использованной работы. Многие имеют хорошую зрительную память. Прочитав несколько работ, дипломник или аспирант начинает писать свою статью, непринужденно излагая чужие мысли и факты в полной уверенности, что теперь это его собственные знания. Так возникает иллюзия авторства. С проявлением «наивного» плагиата второго типа (завороженность чужим текстом) приходится сталкиваться тогда, когда на вопрос: «Почему Вы привели фрагменты из работы автора Х, но не указали, что это не Ваш текст?» можно услышать наивное объяснение: «Там так хорошо и точно все сказано. Я вот именно так и хотел сказать». Таких случаев немало, а ответы выглядят достаточно искренними для того, чтобы выделить эти случаи в самостоятельный подвид.

Мы считаем важным подчеркнуть, что неосознанный плагиат все равно остается плагиатом и не согласны с мнением, что «украденный» текст нередко не является неэтичным заимствованием. Не надо путать причины и совершенное действие. Присвоение контента может происходить по многим причинам, и их так много, что они даже могут подвергаться систематизации по разным признакам: объективные и субъективные, поверхностные и глубинные, «социально-экономические, социально-психологические, культурно-воспитательные, организационно-управленческие и информационно-технологические» [19]. Однако по какой бы причине ни произошло заимствование чужого – оно остается таковым. Метафоры часто опасны при сравнении схожих явлений в разных сферах, но все же для подтверждения этого тезиса сравним плагиат с кражей чего бы то ни было. В юридическом контексте кража квалифицируется как хищение чужого имущества и всегда наказуема с разницей в формах наказания в зависимости от обстоятельств. Например, в соответствии со статьей 146 Уголовного кодекса РФ присвоение авторства (плагиат), если это деяние причинило крупный ущерб автору, наказывается штрафом, исправительными работами или арестом.

Разновидности умышленного плагиата в предлагаемой нами классификации вряд ли нуждаются в комментировании. Отметим лишь, что студенты, осознанно прибегающие к присвоению чужих работ, всегда осведомлены о том, что это неправильно, что должны быть ссылки, что рерайт также предполагает указание источника, поскольку исключает манипуляции с фактическим материалом, терминологией и нередко требует повторения стилистики оригинального текста.

ЦИТИРОВАНИЕ КАК РАЗНОВИДНОСТЬ ЗАИМСТВОВАНИЯ. НАРУШЕНИЕ ПРАВИЛ ПРИВЕДЕНИЯ ЦИТАТ

Являясь промежуточным звеном между плагиатом (явным присваиванием чужого текста без ссылки на автора и источник) и рерайтом (пересказыванием чужого текста и публикацией его под своим именем), цитата обладает значительным манипулятивным потенциалом. Разорванный текст (даже с применением

специальных обозначений) способен исказить представление о событии, формируя ложную медиакартину реальности. Ошибочно переведенная с одного языка на другой цитата становится опасной, особенно если будет использоваться в медицинской или технической сфере. Вырванная из контекста произведения, она может отрицательно сказаться на имидже автора.

Термин «цитата» трактуется авторами большинства словарей одинаково: точная дословная выдержка из какого-нибудь текста, иногда – с указанием на правила оформления, например: «Цитата по правилам русской пунктуации заключаются в кавычки, при цитировании указывается источник цитаты (автор, произведение)» [20]. Правда, некоторые из этих авторов, признавая, что цитата – это «дословное воспроизведение чужой речи» и что «неполнота оформления цитаты, как правило, не допускается в научных и официально-деловых текстах, которые требуют особой точности при воспроизведении чужой речи», отмечают, что «в письменной речи указание на авторство и источник могут отсутствовать, но графическое выделение цитаты в таком случае обязательно» [21]. С последним утверждением сложно согласиться, и оно лишь иллюстрирует наметившуюся тенденцию к ослаблению этических норм использования чужого контента в своих целях. Право автора на имя закреплено в законе, а произведение может существовать в разных редакциях и вариантах, поэтому указание на источник необходимо.

В настоящем исследовании мы исходим из того, что этичные заимствования в форме цитирования – это приведение фрагментов чужого текста с соответствующей ссылкой на источник. Цитирование, т. е. воспроизведение в авторском тексте фрагментов (вербальных и визуальных) различных публикаций с их точной характеристикой, – важный показатель информационной культуры. С нашей точки зрения, цитирование (еще раз отметим – грамотное, адекватное) в сегодняшних условиях становится маркером даже личностных качеств исследователя: определяет вектор его морально-этических представлений, когнитивную адекватность, эрудицию. Вместе с тем очевидно, что при цитировании могут совершаться столь разные ошибки, что некоторые из них воспринимаются как явное нарушение этики. Описание наиболее распространенных ошибок цитирования и погрешностей, возникающих при приведении цитат, поможет преподавателям, учащимся, молодым исследователям контролировать концептуально важный при выполнении квалификационных работ процесс использования информации (рис. 2).

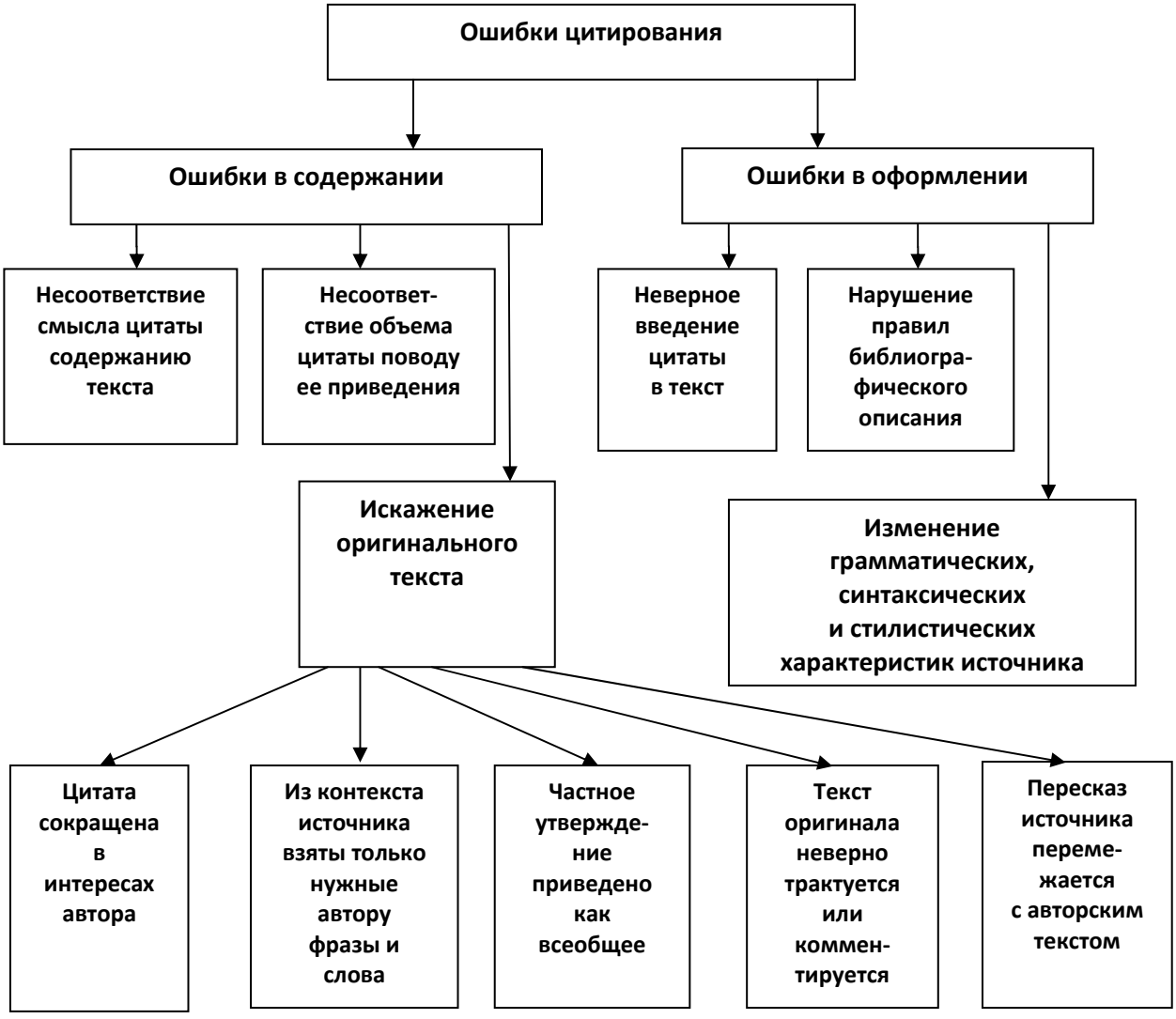


Рис. 2. Основные ошибки цитирования

Выполняя систематизацию ошибок цитирования, мы учитывали некоторые «диагнозы», предложенные А.Э. Мильчиным в книге «Методика редактирования текста» [22].

Наиболее часто встречаются ошибки в содержании. Они возникают прежде всего из-за отсутствия аналитических навыков, умения работать с контентом, но среди прочего – и из-за незнания правил цитирования. Далеко не единичны случаи, когда, например, за достаточной для логики изложения текста констатацией «цифровые медиа занимают лидирующие позиции» идет цитата объемом в страницу, в которой подробно описывается, почему они лидирующие, какие позиции и пр.

Искажение оригинального текста – самый коварный и, пожалуй, разнообразный по числу погрешностей подвид ошибок цитирования, вызванный многими просчетами. На схеме (см. рис. 2) представлены только основные. Например, цитата обрывается в том месте, где заканчивается нужное по смыслу высказывание, хотя при обращении к источнику нетрудно обнаружить, что у этой фразы было другое содержание. Похожая ошибка возникает в том случае, когда из контекста вырывают отдельные словосочетания, нередко окрашенные негативно или, напротив, содержащие высокую оценку, но они вводятся в квалификационную работу применительно вовсе не к тем объектам и ситуациям, которые имел в виду автор цитируемой публикации. Ошибки неверной интерпретации оригинала часто допускаются даже при введении цитаты в учебное сочинение, например: «автор М убежден/утверждает, что…». Если обратиться к оригиналу, то оказывается, что автор М всего лишь высказал предположение. Могут быть и развернутые комментарии, неверно трактующие смысл первоисточника.

Наконец, ошибка пересказа, т. е. использования косвенной цитаты одновременно с прямой (напомним, что в отличие от прямых косвенные цитаты не предполагают кавычек и точного воспроизведения оригинала). Так, автор квалификационной работы хочет замаскировать объемную цитату, но не может по ряду причин (из-за того, например, что его собственный словарный запас гораздо беднее) отойти от оригинала, поэтому что-то в своем тексте воспроизводит на уровне собственного понимания и в своей стилистической манере, что-то – закавычивает. В таком пересказе очень часто слова, обороты, синтаксические конструкции заменяются столь произвольно, что – не всегда преднамеренно – смысл сильно искажается.

Остановимся на одной, казалось бы, безобидной ошибке в оформлении цитаты. Это вмешательство в цитату на языковом уровне. Изменение грамматических и иных характеристик чужого текста совершенно недопустимо. Часто это происходит из желания подогнать цитату под определенную синтаксическую конструкцию, встроить ее в уже написанный текст, который нежелательно менять. Например, в оригинале было написано: «Цитата должна объективно передавать ту мысль, которую вкладывал в нее автор», а в измененном варианте эта же фраза будет выглядеть так: «Существует правило, что «в цитатЕ должна объективно передаватьСЯ тА мысль, которую…».

Приведенная нами систематизация ошибок в цитировании не должна рассматриваться как окончательная. В реальности видов ошибок гораздо больше, они могут классифицироваться по другим основаниям, включать иные разновидности. Предложенные в нашем исследовании схемы (см. рис. 1 и 2) фиксируют попытку структурировать и визуализировать те погрешности, которые встречаются в квалификационных работах разного уровня. Этот шаг крайне важен на пути к этичному, качественному, грамотному использованию информации, которое обязательно должно формироваться в процессе обучения и создания аналитических и исследовательских работ.

ЗАКЛЮЧЕНИЕ

Расширение сферы влияния медиаресурсов привело к изменению не только типа коммуникации (технологический аспект), но и самого человека (психологический аспект). Пандемия ускорила развитие дистанционных коммуникаций, породила социальную интровертность, следствием которой стала частичная десоциализация, а вернее – новый тип социализации, в основе которой не привычное общение, а массово-межличностная сетевая коммуникация.

Современный человек тратит на пользование традиционными и новыми медиаресурсами в среднем около десяти часов ежедневно, из них более семи часов приходится на Интернет. Дистанционные коммуникации, в том числе и онлайн-обучение, повышают время пребывания в сети, в результате чего к медиаповедению уже можно отнести не только то, что человек делает по отношению к медиаресурсу, но и то, чего он не делает [23] .

Сегодня молодые исследователи получают и распространяют контент, часто ориентируясь, в первую очередь, на скорость и легкость доступа к ресурсу, а не на соблюдение традиционных академических правил, основанных на уважительном отношении к интеллектуальной собственности, корректном использовании информации, ответственности за создаваемое произведение. В результате страдают не только имидж самого автора и репутация вуза, но и потребитель медиатекста, введенный в заблуждение сведениями, искаженными из-за неверного цитирования.

Наше исследование показало, что получающий квалификацию специалист склонен самостоятельное знание подменять компилятивной информацией или откровенным заимствованием. Это требует от академического сообщества выработки механизмов противодействия такой тенденции. Одной из простых мер здесь может и должно стать усиление контроля за использованием информации в учебных и исследовательских работах. Имеется в виду не совершенствование существующих программ проверки на антиплагиат, а повышение требований к качеству библиографического аппарата по всем параметрам. Реальная

активность ссылок, релевантность (тематическая, хронологическая, содержательная) используемых источников, выполнение правил библиографического описания – всё это характеризует культуру исследовательской работы, а значит и информационную культуру учащегося и обязательно для освоения.

Специальные курсы и семинары, охватывающие тематику заимствования текстов, должны включать разделы, связанные с изучением особенностей текста, в том числе креолизованного, раскрывать методику аналитико-синтетической переработки информации, обеспечивать развитие логической культуры и языковой грамотности, а также умения организовывать работу с большими объемами информации. Эти курсы целесообразно вводить с первых дней обучения в качестве обязательных, а не факультативных, повторяя некоторые разделы на последующих этапах, постепенно усложняя теоретический материал и уровень практических заданий. Полученные знания и приобретенные навыки помогут учащимся структурировать нужную информацию, а также оперативно принимать решения о возможности и необходимости дальнейшего использования извлеченных сведений.

СПИСОК ЛИТЕРАТУРЫ

1. Четыре закона экологии Барри Коммонера. – URL: https://ecologynow.ru/knowledge/tehnologii-i-ekologia-goroda/cetyre-zakona-ekologii-barri-kommonera (дата обращения 25.01.2022).
2. Ушков П.Ю., Феданов А.Н., Хорошилов А.В. Некорректное заимствование текстов на естественном языке как проявление академической недобросовестности // Открытое образование. – 2006. – № 4. – С. 27-33. – URL: https://cyberleninka.ru/article/n/nekorrektnoe-zaimstvovanie-tekstov-na-estestvennom-yazyke-kak-proyavlenie-akademicheskoy-nedobrosovestnosti/viewer (дата обращения 25.01.2022).
3. Липски С.А. О заимствовании чужого материала в науке и учебном процессе (в порядке дискуссии) // Высшее образование в России. – 2014. – № 6. – С. 101–107. – URL: https://vovr.elpub.ru/jour/article/view/675 (дата обращения 25.01.2022).
4. Плещенко В.И. О плагиате в научных публикациях и выпускных работах // Высшее образование в России. – 2018. – № 8-9. – С. 62-70. – URL: https://cyberleninka.ru/article/n/o-plagiate-v-nauchnyh-publikatsiyah-i-vypusknyh-rabotah (дата обращения 25.01.2022).
5. Севастьянов Д.А. Плагиат в современном образовании: беда или симптом? // Высшее образование в России. – 2017. – № 3(210). – С.17-25. – URL: https://cyberleninka.ru/article/n/plagiat-v-sovremennom-obrazovanii-beda-ili-simptom/viewer (дата обращения 25.01.2022).
6. Ефимова Г.З. Анализ основных стратегий борьбы с проявлениями недобросовестности в науке и образовании. – URL: // https://cyberleninka.ru/article/n/analiz-osnovnyh-strategiy-borby-s-proyavleniyami-nedobrosovestnosti-v-nauke-i-obrazovanii/viewer (дата обращения 25.01.2022).
7. Иншакова Н.Г., Панкеев И.А. Сетевая библиотека как филологический феномен // Филологические науки. Научные доклады высшей школы. – 2020. – № 4. – С. 114-122.
8. Панкеев И.А., Тимофеев А.А. Научное произведение в аспекте деонтологии // Научно-техническая информация. Сер. 1. – 2018. – № 12. – С. 1-7; Pankeev I.F., Timofeev A.A. Scientific Work in the Aspect of Deontology // Scientific and Technical Information Processing. – 2018. – Vol. 45, № 4. – P. 258-264.
9. Панкеев И.А., Иншакова Н.Г. Редактирование научного произведения: нормативно-правовые аспекты // Научно-техническая информация. Сер. 1. – 2019. – № 7. – С. 22-25.
10. Иншакова Н.Г. Информационно-аналитические навыки учащегося вуза // Alma mater. Вестник высшей школы. – 2017. – № 8. – С. 59-63.
11. ГОСТ Р 7.0.100-2018 Библиографическая запись. Библиографическое описание. Общие требования и правила составления. – URL: https://docs.cntd.ru/document/1200161674 (дата обращения 25.01.2022).
12. Толковый словарь Кузнецова. – URL: https://gufo.me/dict/kuznetsov/ (дата обращения 25.01.2022).
13. Плагиат. – URL: Большой энциклопедический словарь. – URL: https://gufo.me/dict/law/%D0%BF%D0%BB%D0%B0%D0%B3%D0%B8%D0%B0%D1%82 (дата обращения 25.01.2022).
14. Плагиат. – URL: https://ru.wikipedia.org/wiki/%D0%9F%D0%BB%D0%B0%D0% B3%D0%B8%D0%B0%D1%82 (дата обращения 25.01.2022).
15. Плагиат. – URL: https://ru.wikipedia.org/wiki/%D0%9F%D0%BB%D0%B0%D0%B3%D0%B8% D0%B0%D1%82 (дата обращения 25.01.2022).
16. Меркулова О.П., Даниленко А.С. Психологические предпосылки студенческого плагиата // Высшее образование в России. – 2014. – № 4. – С. 114-121. – URL: https://cyberleninka/article/n/psihologicheskie-predposylki-studencheskogo-plagiata/viewer (дата обращения 25.01.2022)
17. Plagium vulgaris: как предотвратить плагиат в науке. – URL: http://pressmia.ru/pressclub/20110131/328762171.html (дата обращения: 25.01.2022).
18. Ожегов С.И., Шведова Н.Ю. Толковый словарь русского языка. – URL: https://classes.ru/all-russian/russian-dictionary-Ozhegov-term-36552.htm (дата обращения 25.01.2022).
19. Ефремова Г.З., Кичерова М.Н. Анализ причин академического мошенничества. – URL: https://cyberleninka.ru/article/n/analiz-prichin-akademicheskogo-moshennichestva-i-ih-klassifikatsiya (дата обращения 25.01.2022).
20. Азимов Э.Г., Щукин А.Н. Новый словарь методических терминов и понятий (теория и практика обучения языкам). – Москва: Изд-во ИКАР, 2009. – С 345.

21. Сковородников А.П. Словарь по риторике, языкознанию и эффективному общению. – URL: https://didacts.ru/slovari/slovar-po-ritorike-jazykoznaniyu-i-effektivnomu-obscheniyu.htm
22. Мильчин А.Э. Методика редактирования текста. Изд.3-е, перераб. и доп. – Москва: Логос, 2005. – С.309-311.
23. Жилавская И.В. Медиаповедение личности. Обретение смысла // Медиаскоп. – 2011. – Вып. 2. – URL: http://www.mediascope.ru/node/786 (дата обращения 25.01.2022).

Материал поступил в редакцию 03.02.22.

Сведения об авторах

ИНШАКОВА Наталия Григорьевна – кандидат филологических наук, доцент кафедры теории и методики редактирования факультета журналистики Московского государственного университета им. М.В. Ломоносова
e-mail: inshakovamgu@yandex.ru

ПАНКЕЕВ Иван Алексеевич – доктор филологических наук, профессор факультета журналистики Московского государственного университета им. М.В. Ломоносова
e-mail: iap56@mail.ru

ДЛЯ ЗАМЕТОК