УДК 330.341.11

# ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ЦИФРОВИЗАЦИЯ В КАПИТАЛИСТИЧЕСКОЙ ЭКОНОМИКЕ: ПРОБЛЕМЫ, ВЫЗОВЫ, РИСКИ И ВОЗМОЖНОСТИ

***А.И. БАБЕНКО, преподаватель кафедры экономического анализа, статистики и финансов, Кубанский государственный университет***
*e-mail: bain@inbox.ru*

***И.В. БАБЕНКО, кандидат экономических наук, доцент, доцент кафедры экономического анализа, статистики и финансов, Кубанский государственный университет***
*e-mail: bain@inbox.ru*

**Аннотация**

Применение искусственного интеллекта и цифровых технологий в экономике и жизни сегодня стало важнейшим актуальным трендом. Значимым становится вопрос о возможностях и рисках, возникающих в процессе цифровизации. Авторами рассмотрены аспекты и различные последствия внедрения цифровых технологий в капиталистической экономической системе с учётом особенностей её функционирования.

***Ключевые слова:*** *цифровизация, цифровая экономика, компьютеры, электронно-вычислительные машины, искусственный интеллект, Интернет, капитализм*.

**DOI: 10.31429/2224042X_2024_73_16**

На сегодняшний день темпы и объёмы внедрения технологий, связанных с цифровизацией, непрерывно нарастают. Компьютеры (электронно-вычислительные машины), Интернет, сети связи и нейросети искусственного интеллекта — всё это становится привычным и актуальным, проникая во все сферы жизни. Но что же предлагает применение таких технологий в современном обществе в будущем?

Применение любых технологий, изменяющих технический способ общественного материального и нематериального производства, нельзя рассматривать в отрыве от непосредственно экономической и отношенческой организации данного производственного процесса.

Капитализм — экономическая система, в которой широко распространена частная собственность на факторы производства, а распределение произведённого продукта, товаров, благ, услуг осуществляется в основном посредством рынка [10].

Как известно, при капиталистическом способе организации хозяйственной деятельности мотивационным фактором выступает прибыль индивидуального предпринимателя или коллективного хозяйствующего субъекта.

Для достижения обозначенной цели субъект экономической деятельности применяет все доступные ему средства, по крайней мере, являющиеся законными и возможными к осуществлению и внедрению.

В процессе исторического цивилизационного развития выделяют четыре промышленных революции как основные вехи трансформации хозяйственного процесса [15].

Первая промышленная революция была связана с собственно началом развития производств и добычи угля, а вторая — с изобретением электрической энергии. Эти две промышленные революции произошли очень давно, и их результаты воспринимаются сегодня как сами собой разумеющиеся. Гораздо актуальнее и интереснее с позиций анализа происходящих сегодня в мировой экономике событий выглядят третья и четвёртая промышленные революции.

Третья промышленная революция связана с изобретением и появлением компьютерной, электронно-вычислительной техники. Ее началом считают 1960-е гг. Компьютер является программируемой машиной, позволяющей задавать и автоматически исполнять цепочки операций, а также обрабатывать большие последовательности данных. Иными словами,

компьютер (электронно-вычислительная машина) — это комплекс технических (аппаратных) и программных средств для обработки информации, вычислений, автоматического управления [16]. Его свойства обусловили появление качественно новых возможностей во многих областях человеческой индивидуальной и общественной жизнедеятельности.

Производительность и возможности компьютеров постоянно увеличивались. Известному бизнесмену Биллу Гейтсу, основателю компании «*Microsoft*», приписывают сказанные в своё время слова: «640 килобайт оперативной памяти хватит каждому». Сегодня даже бюджетные ноутбуки, а также мобильные устройства — смартфоны оснащаются 4 гигабайтами (4 × 1 024 × 1 024 = = 4 194 304 Кб) оперативной памяти. Компьютеры более высокого технического уровня оснащаются ещё в 4—16 раз большим объёмом ОЗУ, т. е. от 16 до 64 Гб на один компьютер. Стало повседневным применение многоядерных и многопоточных микропроцессоров, позволяющих эффективно осуществлять многозадачную работу программных продуктов.

Например, шахматный суперкомпьютер «*Deep Blue*» производства корпорации «*IBM*», являвшийся уникальной установкой производства 1997 г., имел производительность, равную 11,38 гигафлопса [21]. Процессор «*i*7-3770K» производства компании «*Intel*», вышедший на рынок в 2012 г., имел в 3 раза бóльшую производительность [19], по данным Калифорнийского университета в Беркли составлявшую 33,26 гигафлопса, при этом он был обычным повседневным продуктом для домашних и рабочих ПК.

Параллельно с развитием самих компьютерных устройств и их программного обеспечения изменялись и каналы связи. Первоначально применялись довольно медленные и ограниченные в пространстве локальные сети, а перемещение данных в основном осуществлялось на физических носителях: флоппи-дисках, магнитных лентах стримеров, а затем и *CD* / *DVD*-дисках оптического типа. Затем появились новые виды физических носителей данных: *USB-flash*-накопители, с течением времени заметно увеличившие объемы памяти и потерявшие в цене, а

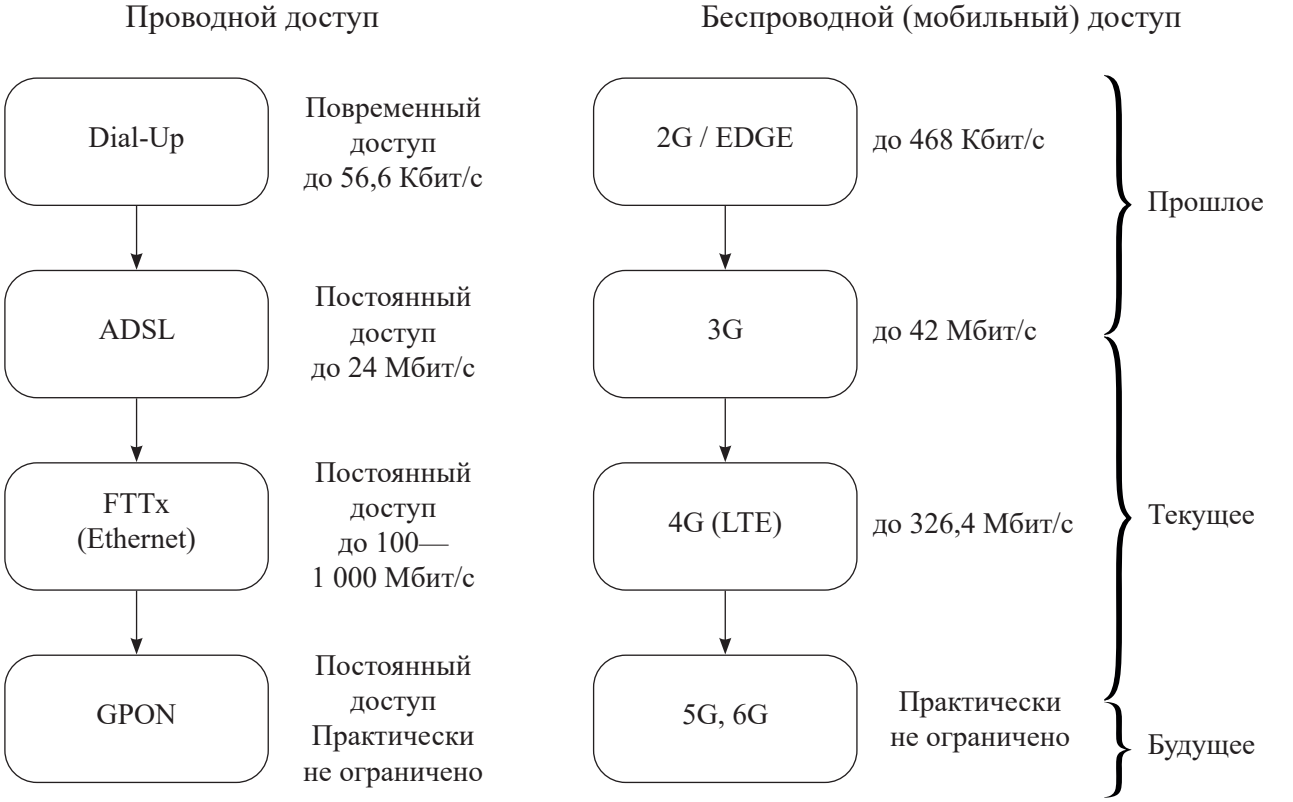


Рис. 1. Эволюция средств доступа к сети Интернет (составлен авторами)

также высокоёмкие, но дорогостоящие оптические диски *HD-DVD* и *Blu-Ray*. Однако настоящим качественным преобразованием средств перемещения и обмена информацией стало распространение и развитие глобальной инфокоммуникационной сети Интернет. Нами составлена схема развития технологий беспроводного и проводного доступа к глобальной сети (рис. 1).

Таким образом, появился Интернет как глобальная сеть, объединяющая расположенные в самых разных странах мира, от США до КНДР, компьютеры. Возможности и скорость доступа к глобальной инфокоммуникационной сети постоянно возрастали. Например, скорость самых производительных современных видов доступа к Сети (1 Гбит/с) уже как минимум сравнима с производительностью чтения/записи данных с традиционных жёстких дисков, т. е. доступ к содержащейся в Сети информации возможен на скорости, с которой ранее осуществлялся только к локально хранящимся данным. А для передачи и получения по сетевому подключению 1 Гбит/с всех данных, хранящихся на одном оптическом машинном носителе формата *DVD* (4,7 Гбайт), потребуется менее одной минуты, что быстрее, чем понадобилось бы для чтения такого же объема данных локально с диска *DVD* (однократная скорость работы *DVD*-дисковода составляет около 11 Мбит/с, у современных дисководов скорость чтения обычно 24-кратная, что составляет около 265 Мбит/с) или с *flash*-накопителя *USB* 2.0 (до 480 Мбит/с).

Динамика числа пользователей Интернета в России представлена на рис. 2.

По данным Организации Объединённых Наций (ООН), 4,9 млрд людей в мире — пользователи Интернета, таким образом, глобальная инфокоммуникационная сеть стала явлением, затрагивающим жизнь большинства людей (рис. 3).

Все сказанное обусловило начало четвертой промышленной революции, которая понимается как обильное внедрение искусственного интеллекта, интернет-технологий и т. д.

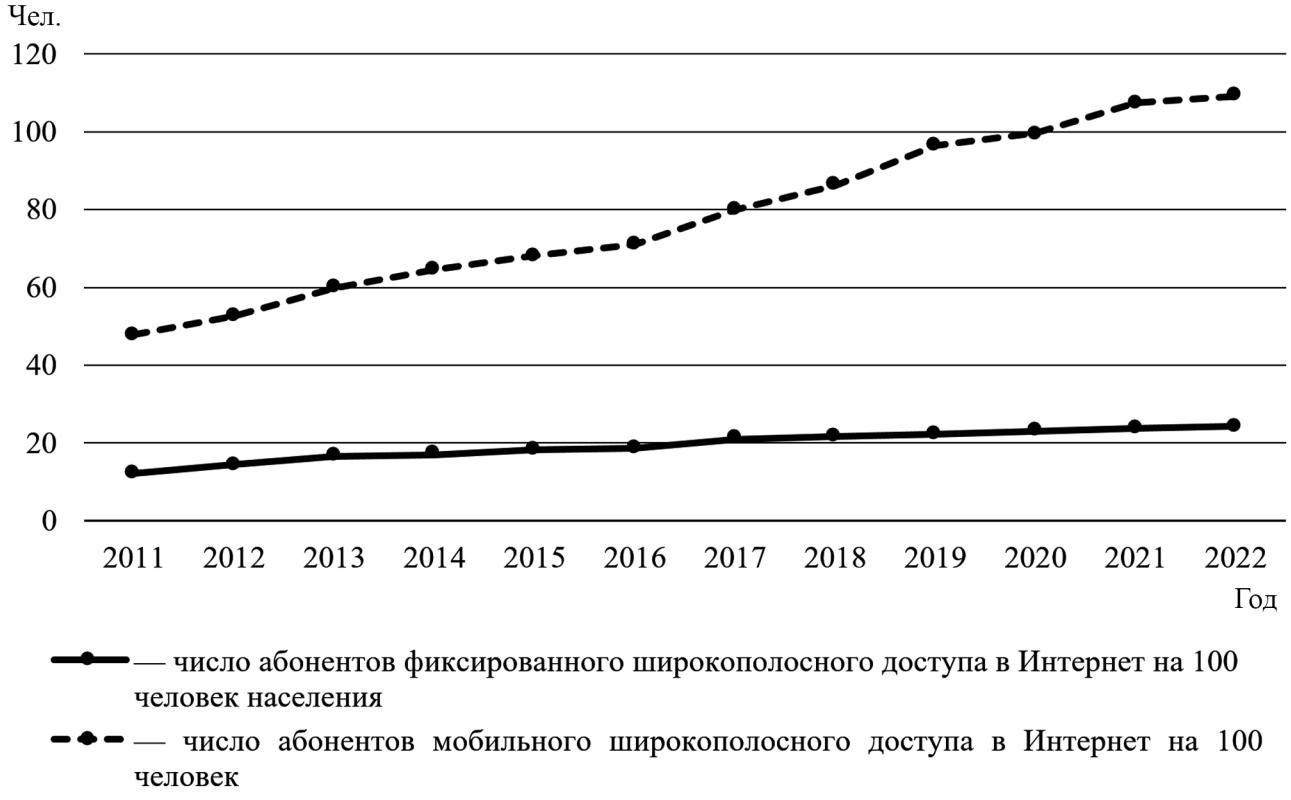


Рис. 2. Динамика числа пользователей глобальной инфокоммуникационной сети Интернет (составлен авторами по [19])

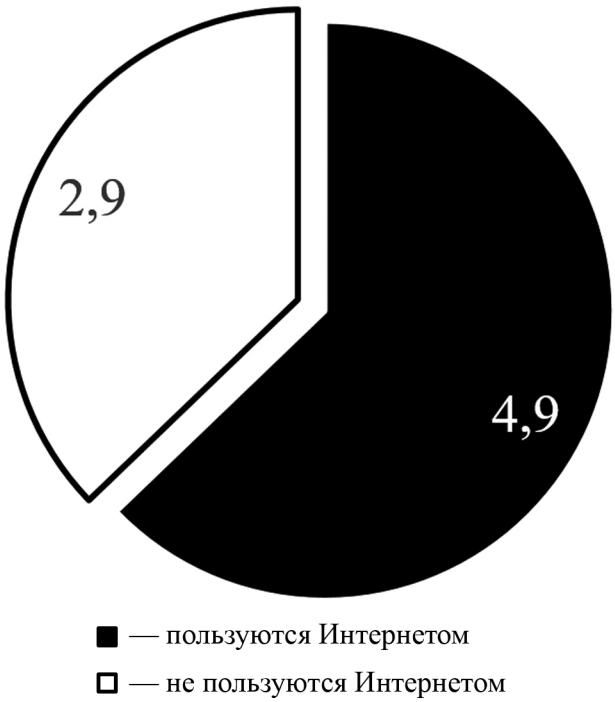


Рис. 3. Численность пользователей Интернета среди населения мира, млрд чел. (составлен авторами по [2])

Нами дано общее описание всех 4 промышленных революций (рис. 4).

Сегодня появляются программные продукты и ресурсы, которые предоставляют ранее невиданные возможности. В числе наиболее актуальных направлений можно обозначить:

– биометрические системы: позволяют идентифицировать людей по голосу, лицу и иным признакам;

– основанные на искусственном интеллекте, нейросетях чат-боты: позволяют поддерживать беседу с компьютером с ответами на различные вопросы; наиболее известным программным комплексом такого рода является *ChatGPT*; он позволяет формулировать самые разные запросы: написание программных кодов и текстов, анализ разных файлов и ответы на вопросы по ним (*ChatPDF*) и др.;

– основанные на нейросетях системы генерации визуальных образов; наиболее известными продуктами такого рода являются *Midjourney*, *Stable Diffusion*, *Fusion Brain* (*Kandinsky*); функционал данных продуктов позволяет создавать изображения, содержащие визуализацию с заданными свойствами, например, исходя из текстового описания-запроса содержания создаваемого рисунка;

– иные системы различного назначения и функционального содержания.

Каковы же достоинства и недостатки внедрения подобных систем и продуктов, а также риски их имплементации в повседневную социально-экономическую жизнь при капиталистическом типе хозяйствования?


Рис. 4. Промышленные революции в истории мирового экономического хозяйства (составлен авторами)

Нами выделены позитивные и негативные возможные последствия внедрения систем искусственного интеллекта и цифровизации, представленные в таблице.

Рассмотрим более подробно возможности, предоставляемые цифровыми системами: повышение производительности труда; независимость процессов от антропогенных факторов; неотвратимость наказаний и отсутствие отклонений от установленного алгоритма действий; практически неограниченные возможности по агрегации, обработке и передаче данных.

1. Повышение производительности труда. Применение новых систем позволяет быстрее осуществлять многие хозяйственные операции. К тому же искусственный интеллект не склонен при исправном функциональном состоянии аппаратного и программного обеспечения совершать ошибки, «отлынивать от работы» и т. д. Все это заметно повышает возможности по получению прибавочной стоимости. Однако критическим будет вопрос о дальнейшем справедливом распределении данной прибавочной стоимости. В противном случае общество не получит полезного эффекта. Напротив, социуму может быть даже нанесён вред за счёт сокращения спроса на рынке труда, что будет рассмотрено далее. Различия исполнителей (человека и машины) представлены на рис. 5.

2. Независимость процессов от антропогенных факторов. Искусственный интеллект позволяет совершать действия, не привязываясь к субъективным свойствам исполнителя действия: его желаниям, настроениям, ошибкам и т. д. Тем не менее важно помнить, что у любой системы есть владелец и администратор, и последствия их действий могут быть катастрофическими по масштабам.

3. Неотвратимость наказаний и отсутствие отклонений от установленного алгоритма действий. Система искусственного интеллекта способна обеспечить выполнение поставленных задач при условии, что таковые действительно заложены в её программный код должным образом. Также стоит отметить, что подобное поведение систем и общества под их контролем приводит к фактической ликвидации такого эволюционного механизма развития, как изменчивость, что будет рассмотрено далее.

4. Практически неограниченные возможности по агрегации, обработке и передаче данных. Современные цифровые системы позволяют оперативно структурировать и связывать в единое целое огромные массивы данных из различных (гетерогенных) источ-

Позитивные и негативные последствия внедрения систем искусственного интеллекта и цифровизации (составлена авторами)

| Тип последствий | Последствия |
|---|---|
| Позитивные последствия (возможности) | Повышение производительности труда |
| | Независимость процессов от антропогенных факторов |
| | Неотвратимость наказаний и отсутствие отклонений от установленного алгоритма действий |
| | Практически неограниченные возможности по агрегации, обработке и передаче данных |
| Негативные последствия (риски) | Утечка данных |
| | Тоталитарный контроль политической и экономической власти над обществом |
| | Закрытые алгоритмы |
| | «Избыточная» интеграция и агрегация данных |
| | Утрата вариативности поведения субъектов |
| | Потеря возможности заработка и рост безработицы |
| | Подмена и фальсификация данных |
| | Биометрическая фальсификация |


Рис. 5. Зависимость исполнения алгоритма осуществления процесса от типа исполнителя (составлен авторами)

ников. Но данный факт может также вести к отрицательным последствиям, которые будут рассмотрены далее.

Перечисленные достоинства — важные характеристики цифровых систем. Но не менее очевидны и риски их применения. Особенно ярко эти риски, на наш взгляд, проявляются именно в капиталистическом типе экономического хозяйствования, так как в нем мотивационным фактором выступает увеличение индивидуальной прибыли. В результате даже те качества информационно-вычислительных систем, которые при социалистическом типе хозяйствования, ориентированном на общественную пользу, имели бы преимущественно положительные последствия для общественной деятельности, создают серьёзные угрозы для общества. К основным рискам цифровизации следует отнести 8 рисков.

1. Риск утечки данных. Как показала мировая и российская практика, такой риск неизбежен. Для осуществления самого процесса обработки информации субъекты деятельности должны иметь к ней доступ. Соответственно, как у внутренних субъектов (по данным известного эксперта в области информационной безопасности, президента группы компаний *InfoWatch*, Натальи Ивановны Касперской, большинство утечек данных связаны с действиями сотрудников [4]), так и у внешних субъектов (хакеров) возникает соблазн ради личной выгоды или по каким-либо иным соображениям (например, идеологически или личного самоутверждения) осуществить несанкционированный доступ и распространение информации. Далеко не каждый готов внезапно увидеть фото и видео из личного альбома в «облачном» сервисе, представленные на публичных ресурсах всем любопытным для обсуждения. Известно, что от утечки личных медиаданных, хранимых, в частности, в «облачном» сервисе *Apple iCloud*, пострадали ряд знаменитостей [17]. Появление новых устройств интернета вещей (*IoT — Internet of Things*), который является неотъемлемым элементом концепции IV промышленной революции, многократно

увеличивает этот риск. Видеокамеры наблюдения собирают сведения о передвижениях и поведении граждан, «умные» телевизоры, смартфоны, планшеты и ноутбуки имеют в своём составе встроенные микрофоны и камеры, а подключаемые к глобальной инфокоммуникационной сети Интернет холодильники, унитазы, чайники и медицинские приборы могут многое собрать, хранить и, соответственно, «рассказать» о жизнедеятельности индивида. Все способы защиты данных имеют свои недостатки. В частности, отключение «умного» устройства от инфокоммуникационной сети Интернет приведёт к заметному (а в ряде случаев полному) усечению его функционала, физическое блокирование аппаратных средств получения информации устройства не всегда возможно штатными средствами (например, лишь немногие устройства с веб-камерами имеют штатные шторки для закрытия объектива камеры) и зачастую ограничивает и требуемый функционал (например, применение той же камеры для коммуникации посредством видео-конференц-связи), применение антивирусных программных продуктов не гарантирует 100 % защиты от всех угроз, а применение средств фильтрации входящего и исходящего трафика (*firewall*) является сложным в настройке, не всегда возможно такое ограничение трафика без усечения важного функционала того или иного аппаратного или программного продукта. Всё становится ещё сложнее в случае с принуждением к цифровому хранению данных в информационных системах со стороны государств и корпораций. Тогда отказ гражданина от хранения и обработки данных, если и возможен, то приводит к поражению в правах, вплоть до выхода из дома и приобретения необходимых товаров, как это было в 2020—2022 гг. в связи с «санитарными» ограничениями.

2. Риск тоталитарного контроля политической и экономической власти над обществом. Этот риск является очевидной обратной стороной неотвратимости наказания. Демократические процедуры несовершенны, а цифровой контроль полностью закроет для общества лазейку под названием «закон не прижился». Нельзя не упомянуть и риски, связанные с поведением чисто экономических субъектов, не обладающих, казалось бы, политической властью. Так, блокирование аккаунта в сервисе, фактически занимающем монопольное или олигопольное положение на рынке, может заметно снизить качество жизни и возможности гражданина, в том числе по осуществлению общественной деятельности. Примером могут служить события, происходившие с Дональдом Трампом, занимавшим пост президента США с 20 января 2017 г. по 20 января 2021 г. Аккаунты Дональда Трампа оказались заблокированными во многих глобально значимых инфокоммуникационных сервисах: *Facebook* (сервис компании *Meta*, запрещён в России и признан экстремистской организацией), *Instagram* (сервис компании *Meta*, запрещён в России и признан экстремистской организацией), *Twitter* (запрещён в России) и даже *Snapchat* и *Twitch* [11]. Это фактически привело к «отключению» личности от политической и общественной деятельности, блокированию права на самовыражение, свободу слова и политическую деятельность. Более того, при попытке создания сторонниками Трампа иных новых инфокоммуникационных сервисов, таких как *Parler*, они также столкнулись с блокированием этих программных продуктов в магазинах приложений, таких как *Apple App Store* [18]. Таким образом, «неудобная» точка зрения оказалась изгнана из сервисов, занимающих олигопольное положение на рынке, а новые сервисы получили препятствия от сервисовплатформ, также занимающих олигопольное положение. Известно, что многие инфокоммуникационные продукты принадлежат фактически монопольным или олигопольным рыночным игрокам. На рис. 6 приводятся примеры подобных продуктов.

Иным примером (уже скорее диктатуры политической власти, а не рыночных субъектов) могут послужить меры, связанные с «санитарными» или «климатическими» ограничениями, которые, как известно, являются для общества весьма спорными. В случае тотального внедрения цифровых систем об-

ществу можно будет легко навязать любые ограничения, придуманные узкой властвующей группой. Любое нарушение единогласно установленных политической или экономической властью правил игры будет немедленно отслеживаться и далее назначаться наказание (понижение социального рейтинга, отключение *QR*-кода или биометрического аккаунта для доступа в магазины и общественный транспорт, блокирование аккаунта в сервисе, взыскание штрафа с безналичного или цифрового счета и т. д.).

3. Риск закрытых алгоритмов. Бóльшая часть программных продуктов и сервисов, используемых сегодня в мире, не имеют открытого исходного кода (*open-source*). Проверка фактических алгоритмов систем, например, используемых при проведении дистанционного электронного голосования в различных странах, является затруднительной или невозможной. Известен случай, вызвавший скандал «дизельгейт» (*dieselgate*) с автомобилями немецкого концерна *VAG* (*Volkswagen Audi Group*). Установленное за-

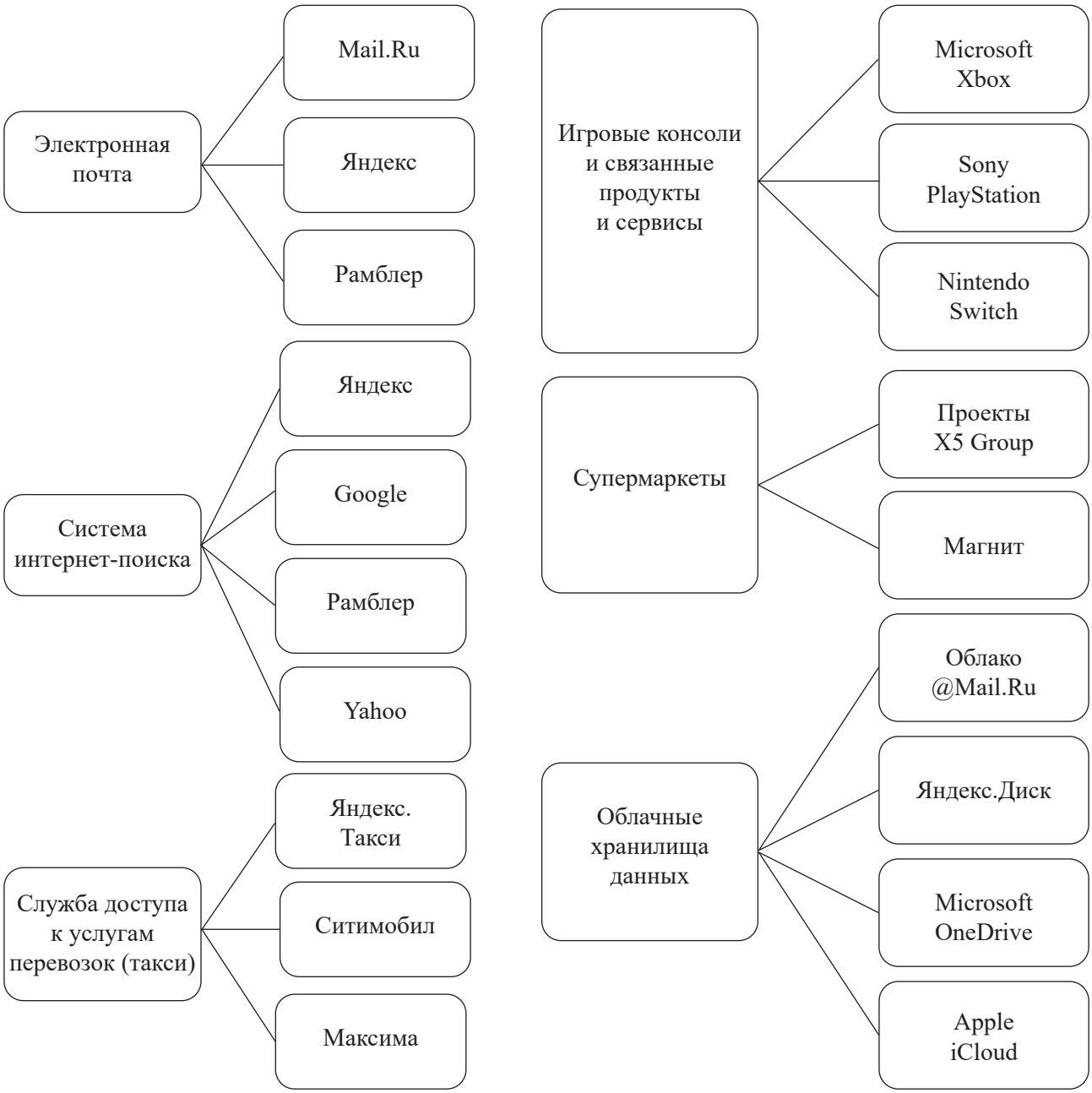


Рис. 6. Примеры олигопольных рынков ИТ- и иных продуктов (составлен авторами)

водом-изготовителем в электронный блок управления (ЭБУ) автомобиля программное обеспечение (ПО) в качестве своего основного функционала контролирует режим подачи в двигатель топливной смеси и режим функционирования двигателя в целом. Разработчик и правообладатель ПО ЭБУ в лице концерна *VAG* предусмотрел в алгоритме незаявленные при получении одобрения типа транспортного средства (ОТТС) в различных странах мира возможности системы. Аппаратно-программный комплекс ЭБУ за счёт скрытых возможностей умел определять факт проведения тестирования автомобиля на специальном стационарном стенде, находящемся на станции технического обслуживания (СТО). При этом в работе ЭБУ активировался специальный режим, приводящий к модификации компьютерной информации выполняемой программы в оперативном запоминающем устройстве (ОЗУ) и смене режима работы двигателя для обеспечения соответствия выхлопа автомобиля обязательным экологическим нормам стран мира. Такой режим работал только при тестировании и не был оптимален по другим параметрам, таким как скоростно-динамические. После выезда же автомобиля с СТО на дорогу и начала реального движения специальный режим ПО отключался и автомобиль приобретал желанные потребительские качества, но переставал фактически соответствовать экологическим нормам. Алгоритм функционирования оригинального, содержащего скрытые возможности, программного обеспечения ЭБУ *VAG* представлен на рис. 7. Это позволило долгое время незаметно для контролирующих органов и общественности выводить на рынок автомобили, фактически не соответствующие в реальной эксплуатации обязательным законодательным экологическим нормативам. Как следствие, производителю пришлось понести репутационные издержки, а также материальные и трудовые затраты на разработку версии ПО, способной обеспечить приемлемые экологические и иные пара-метры работы без использования запрещенных приемов, а также на её установку взамен имеющейся в постоянные запоминающие устройства (ПЗУ) ЭБУ уже выпущенных и реализованных автомобилей [23].

Помимо изначально внесенных в ПО скрытых возможностей случаются и ситуа-

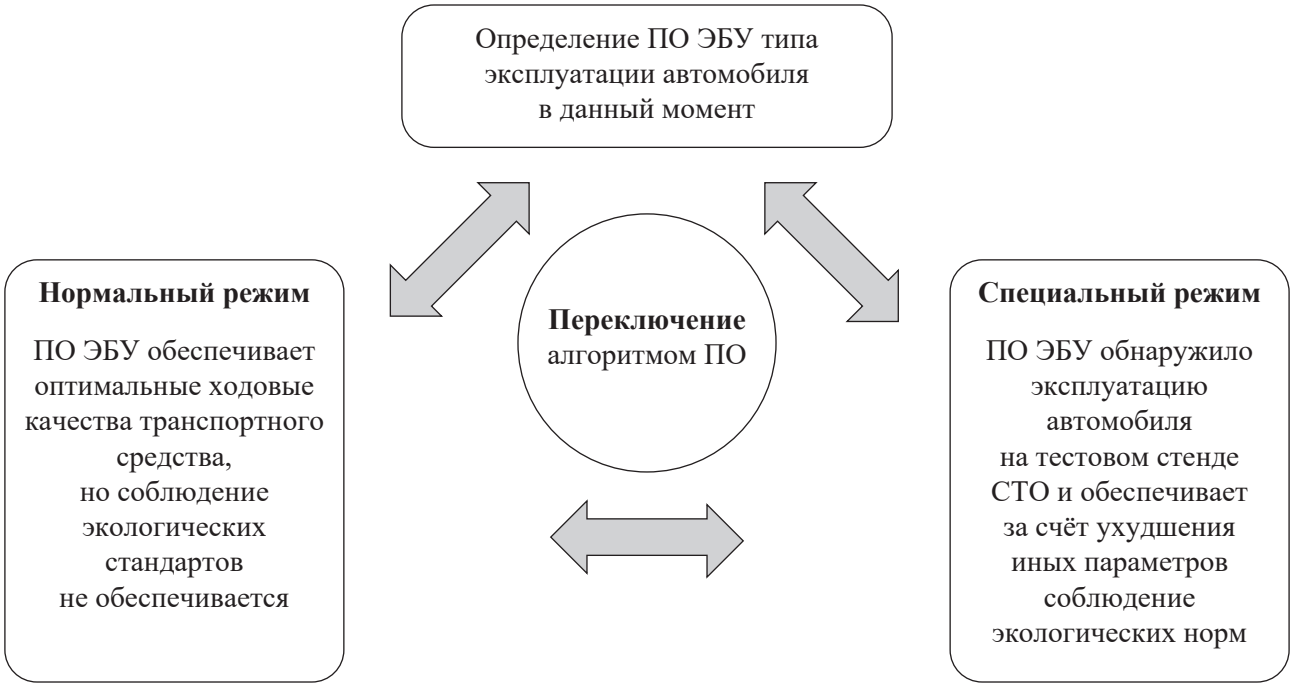


Рис. 7. Алгоритм функционирования ПО ЭБУ *Volkswagen Audi Group* со скрытым функционалом (составлен авторами)

ции, когда ПО модифицируется по сравнению с заложенной при производстве и выпуске в реализацию версией. Такие ситуации будут рассмотрены далее при описании рисков фальсификации данных, хранимых и обрабатываемых в информационных системах.

4. Риск избыточной интеграции и агрегации данных. Основной особенностью реляционных (от англ. *relation* — отношение) баз данных является возможность создания взаимосвязанных друг с другом таблиц данных. Соответственно, достаточно лишь директивного указания, чтобы объединить в единое целое все данные о человеке или ином процессе: из детских садов, школ, полицейских участков, учреждений здравоохранения, магазинов, торговых сетей и т. д. Инфокоммуникационные сети, включая глобальную сеть Интернет, обеспечивают мгновенную передачу и объединение данных из различных (гетерогенных) источников, т. е. технически операция установления любых дополнительных данных о человеке, поиска всех людей или иных объектов по определённым критериям (в том числе множественным пересекающимся) сводится к подаче в информационную систему соответствующих *SQL*-запросов (*Structured Query Language* — «язык структурированных запросов» — декларативный язык программирования, применяемый для создания, модификации и управления данными в реляционной базе данных, управляемой соответствующей системой управления базами данных). Готовы ли люди к тому, что информация, например, полученная из школы, детского сада или медицинского учреждения будет применена при установлении трудовых отношений (например, полученная в 1-м классе оценка повлияет на приём на работу)? Или к применению информации, полученной с видеокамер наблюдения, при заключении кредитного договора или договора медицинского страхования (например, имеющаяся в СУБД видеозапись курения сигареты, или превышения скорости на автомобиле либо мотоцикле, или перехода улицы на запрещающий сигнал светофора приведёт к повышению страховой премии по договору ДМС)? Пример работы механизма агрегации данных приведен на рис. 8.

5. Риск утраты вариативности поведения субъектов. Известно биологическое понятие «изменчивость», которая выступает как важнейшая движущая сила эволюции. Изменчивость — это свойство организмов изменяться, которое состоит в приобретении новых признаков и свойств или в потере тех, которые уже приобретены [14]. Таким образом, речь идёт об адаптационном процессе приспособления. Аналогичные процессы наблюдаются и в социокультурном пласте, являющемся надстройкой над биологическим. Изменение представлений о мироздании, например, о вращении и расположении планеты, равно как и иных, всегда сталкивалось с противодействием. Человеческая культура на протяжении всей многовековой истории (как в узком смысле [произведения искусства и духовной сферы], так и в широком [совокупность всей общественной и цивилизационной деятельности людей]) [3] подвержена влиянию субъективно-личностного фактора как важнейшей движущей силы (рис. 9).

Связанный с риском тоталитарного контроля (описанным ранее), этот риск означает утрату личностного фактора и переход к обществу, лишённому творчества, изменчивости и мыслящему по заданной программе. Такие программы и показатели будут в лучшем случае отражать «усреднённого» человека, не соответствуя потребности в более индивидуализированном внутреннем содержании и блокируя общественную эволюцию и развитие, а в худшем — они будут содержать внутренние смысловые настройки, обслуживающие лишь интересы власть имущих и владельцев капитала. На наш взгляд, особенно опасны в этом плане проекты, связанные с модификацией человека, трансгуманизмом, такие как нейроимплантируемые чипы (нейроимпланты). Подобными исследованиями занимается компания «*Neuralink*», основанная в 2016 г. и принадлежащая известному предпринимателю Илону Маску. Упоминание нейроимплан-

| ID NO. | Вес при рождении, г |
|---|---|
| 001 | 4200 |
| 002 | 4300 |
| 003 | 3980 |
| 004 | 4000 |
| 005 | 4000 |
| 006 | 2999 |

| ID NO. | Балл государственного экзамена |
|---|---|
| 001 | 98 |
| 002 | 63 |
| 003 | 78 |
| 004 | 80 |
| 005 | 90 |
| 006 | 34 |

| ID NO. | Число штрафов за курение |
|---|---|
| 001 | 0 |
| 002 | 0 |
| 003 | 2 |
| 004 | 3 |
| 005 | 5 |
| 006 | 1 |

| ID NO. | Средний чек в супермаркете, р. |
|---|---|
| 001 | 2500 |
| 002 | 1000 |
| 003 | 750 |
| 004 | 800 |
| 005 | 703 |
| 006 | 827 |

| ID NO. | Вес при рождении, г | Балл государственного экзамена | Число штрафов за курение | Средний чек в супермаркете, р. |
|---|---|---|---|---|
| 001 | 4200 | 98 | 0 | 2500 |
| 002 | 4300 | 63 | 0 | 1000 |
| 003 | 3980 | 78 | 2 | 750 |
| 004 | 4000 | 80 | 3 | 800 |
| 005 | 4000 | 90 | 5 | 703 |
| 006 | 2999 | 34 | 1 | 827 |

Рис. 8. Схема агрегации данных из различных источников (гетерогенных данных) с использованием ключевого поля «*ID NO*.» (составлен авторами)

тируемых устройств имеется и в отечественных нормативных документах. В частности, в Приказе Минпромэнерго РФ от 7 августа 2007 г. № 311 «Об утверждении Стратегии развития электронной промышленности России на период до 2025 года» прямо говорится о необходимости применения устройств, характеризуемых как «наноэлектроника», которые должны будут «интегрироваться с биообъектами», производить «непрерывный контроль» за их жизнедеятельностью, основная цель которого — «сокращать социальные расходы государства» [8]. Если программное обеспечение, содержащееся в таких устройствах, сможет напрямую изменять мысли или действия человека, а также получать мысли человека из мозга и обрабатывать их затем в искусственной информационной системе, это приведёт к ликвидации остатков личных свобод граждан, а также возможному навязыванию общественным группам полностью чужеродных для них идей, мыслей, эмоций, приоритетов и способов функционирования. Возникнет такое состояние, при котором «рабство» станет не только неотменяемым, но и даже в принципе не осознаваемым личностью.

Нельзя не отметить в связи с этим риском внедряемые в различных странах цифро-

вые валюты (*CBDC — Central Bank Digital Currency*), которые при внимательном рассмотрении имеют заметные и принципиальные отличия от всех известных ранее форм денег: наличной (*cash*), безналичной (*cashless*) и традиционных криптовалют (*crypto-currencies*), примерами которых являются программные продукты *Bitcoin*, *Bitcoin Cash*, *Ethereum*, *Ethereum Classic*, *Dogecoin* и др. Эволюция форм денег государств представлена на рис. 10.

Наличные деньги не оснащены в принципе никакими средствами прослеживаемости, за исключением номеров купюр и возможности физического нанесения краски на конкретные купюры. Прослеживаемость и управляемость обращения безналичных денег также в заметной степени ограничена. Все денежные единицы, хранимые на безналичном банковском счёте, являются равнозначными. Не существует безналичных денежных единиц «только на еду» или безналичных денежных единиц, которые можно тратить, если, например, не курили перед какой-либо подключённой к общей системе видеокамерой наблюдения в этом месяце или не превысили свой углеродный лимит (*carbon limit*) личного влияния на глобальное потепление. Все возможные ограничения, которые могут быть наложены на безналичный счёт пользователя, носят только системный характер, такой как взыскание долгов. Криптовалюты же в принципе являются децентрализованными и анонимными формами денежного обращения, обеспечивая ещё большую свободу циркуляции по сравнению с безналичными деньгами. *CBDC*-валюты, исходя из определения, имеют единый центр эмиссии и обращения — центральный банк государства, что делает их «антиподом» криптовалют. Внедрение *CBDC*-валюты «*eNAIRA*» в Нигерии вызвало неприятие и протесты со стороны общественности [22]. В РФ также был принят Федеральный закон от 24 июля 2023 г. № 340-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации», закрепивший введение такой формы денег, как цифровой рубль [7]. Данную форму валюты можно считать *CBDC*-валютой. Все это открывает ранее невиданные технические возможности для внедрения программных продуктов, реализующих функционал полного контроля и управ-

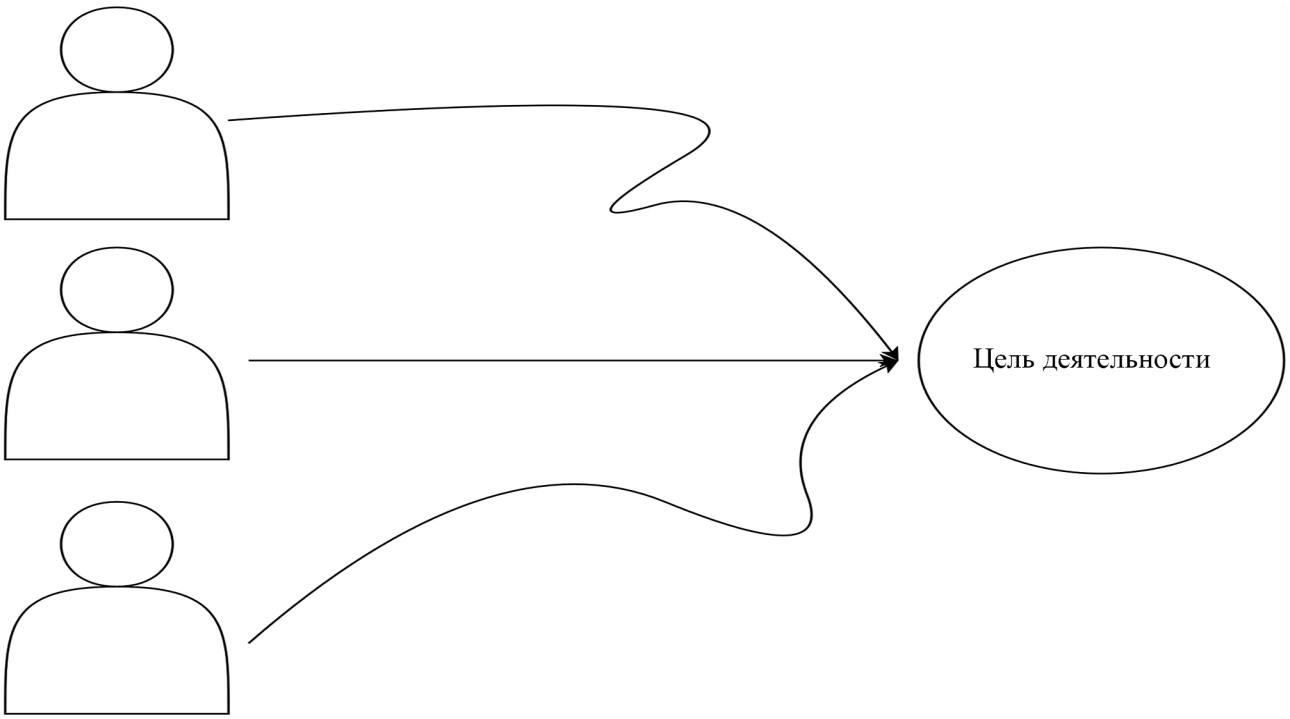


Рис. 9. Изменчивость как способность достижения целей различными путями, из которых в ходе прогресса отбираются самые эффективные (составлен авторами)

ления экономическим поведением каждого гражданина, нужно лишь принятие соответствующих законодательных актов.


Рис. 10. Эволюция современных форм денег государств (составлен авторами)

6. Риск потери возможности заработка и роста безработицы. Автоматизированные системы способны эффективно заменять труд людей, что может привести к стремительному увеличению безработицы. О перспективах замены продавцов, уборщиков, водителей и подобных профессий на автоматизированные средства говорят уже достаточно давно. Например, представленный аппаратно-программный комплекс компании «КамАЗ» способен обеспечить функционирование беспилотных грузовых автотранспортных средств. Согласно описанию аппаратно-программного комплекса достаточно лишь 1 оператора для функционирования 20 беспилотных транспортных средств [9]. Таким образом, произойдет потеря 19 из 20 рабочих мест, что составляет 95 % (рис. 11).

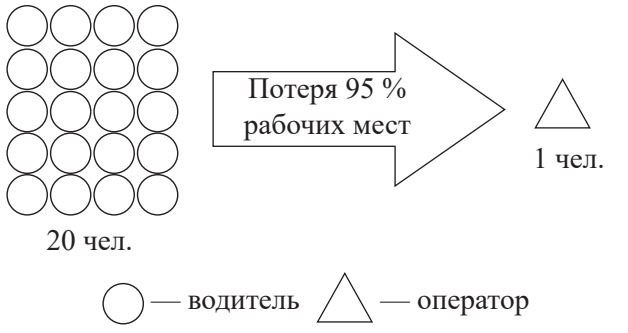


Рис. 11. Утрата рабочих мест при переходе на эксплуатацию беспилотного грузового транспорта (составлено авторами по [9])

Соответственно, произойдёт высвобождение живых трудовых ресурсов, надобность в которых будет снижена или ликвидирована. Нынешние же нейросети открыли потенциал к полной или частичной замене не только водителей, дворников, уборщиков и т. д., но уже и программистов, художников, дизайнеров, преподавателей, врачей и прочих, как считалось ранее, интеллектуальных или творческих профессий.

Системы искусственного интеллекта будут способны сами, функционируя без или с минимальным вмешательством живого персонала, генерировать огромный прибавочный продукт и прибавочную стоимость, но при продолжении капиталистической экономической политики, т. е. без проведения национализации и / или сверхналогообложения (изъятия заметной доли прибавочной стоимости для содержания людей, ставших ненужными в качестве работников), данный прибавочный продукт будет оставаться в распоряжении собственников средств производства (предприятий и эксплуатируемых ими цифровых систем). Возможности же заработка иными лицами, не входящими в данный круг собственников, вероятно, будут резко сокращены (рис. 12).

По данным исследования Росстата, в 2019 г. было выявлено, что примерно половина российских семей испытывает проблемы с приобретением чего-либо помимо еды и одежды, а 15 % недоступна даже одежда [13]. Очевидно, что внедрение описанных механизмов, влекущее «выключение» живых людей из экономической деятельности, приведёт к многократному ухудшению данной ситуации.

Внедрение беспилотных и подобных автоматизированных технологий по очевидным причинам вызывает общественные протесты по всему миру. В частности, известен случай, когда жители города Сан-Франциско (США) помещали пластиковые дорожные конусы на капот самоуправляемых автомобилей такси [1]. Это не приводит к разрушению автомобиля, однако блокирует возможность дальнейшего движения автомобиля, так как аппаратно-программным комплексом распознаётся как нештатная и потенциально опасная ситуация. Тем не менее, на наш взгляд, подобные протесты не являются длительно-социально-оптимальным выходом, необходим пере-

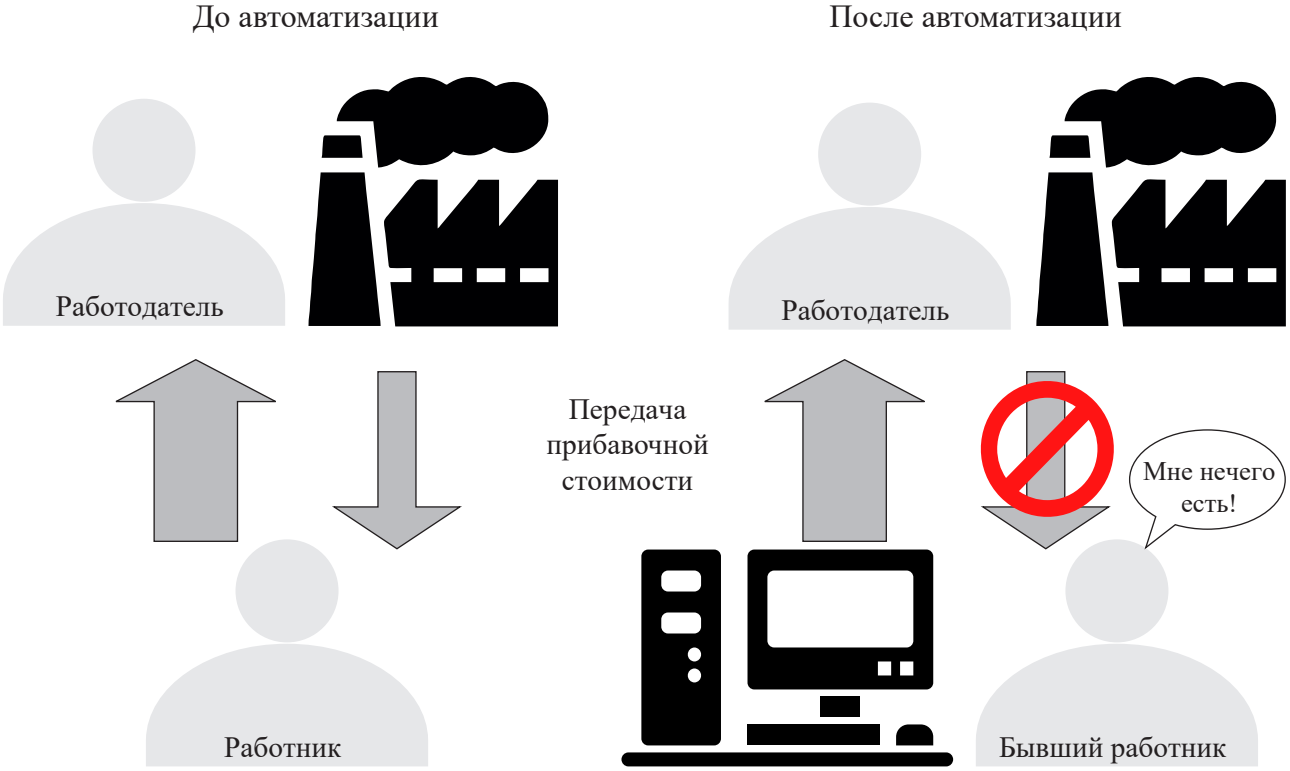


Рис. 12. Изменение трудовых отношений после автоматизации производства путём их уничтожения (составлен авторами)

смотр механизма распределения прибавочной стоимости как такового.

7. Риск подмены и фальсификации данных. Данный риск тесно связан с ранее рассмотренным (риском закрытых алгоритмов. Ранее был приведён пример функционирования программного обеспечения, установленного в автомобилях концерна *VAG*, в котором был реализован скрытый функционал подмены данных о состоянии экологических эмиссий автомобиля. Необходимо заметить, что изменение функционала может быть внесено как изначально, так и на более позднем этапе. Это связано с тем, что наличие права владения и распоряжения информационной системой (ИС) у конкретного субъекта вкупе с отсутствием возможностей полноценного контроля за функционированием ИС со стороны общественности создаёт риски манипуляции поведением ИС со стороны лиц, осуществляющих контроль над работой системы. Одним из примеров ИС, где особенно критична целостность и достоверность обрабатываемой информации, являются массово применяемые в избирательных процессах ИС обработки голосов. Находят применение такие системы и в России, в частности, в виде следующих аппаратно-программных комплексов: «КОИБ» (комплекс обработки избирательных бюллетеней — система автоматического оптического сканирования на избирательном участке заполненных избирателями бумажных бюллетеней), «КЭГ» (комплекс электронного голосования — электронный терминал для голосования на избирательном участке) и «ДЭГ» (дистанционное электронное голосование — волеизъявление с использованием домашнего компьютера).

В статье Седы Давтян с соавторами «*Taking total control of voting systems: firmware manipulations on an optical scan voting terminal*» («Получение тотального контроля над системами голосования: манипуляции над прошивкой оптического терминала сканирования голосов») [20] исследователями была доказана возможность перепрошивки микросхемы постоянного запоминающего устройства (ПЗУ) оптического сканирующего устройства линейки «*AccuVote*» компании «*Diebold*» для осуществления избирательного процесса на

выборах. Без получения разрешения или содействия компании-производителя исследователям в процессе проведения эксперимента удалось создать модифицированную версию операционной системы «*AV-OS*» (*AccuVote Operating System* — операционная система *AccuVote*) и записать её в ПЗУ аппаратно-программного комплекса *AccuVote Optical Scan Terminal* (терминал оптического сканирования *AccuVote* — по функциональному назначению аналогичен «КОИБ»). После установки в ПЗУ модифицированного программного обеспечения, предназначенного для блокирования, уничтожения и модификации легитимной компьютерной информации о голосах избирателей, функция печати и выгрузки в центральную государственную систему стала передавать на принтер и в центральную систему управления базой данных (СУБД) фальсифицированные итоги процедуры голосования, а информация об истинных итогах избирательной процедуры оказалась утрачена.

Тем самым в ходе эксперимента было произведено уничтожение оригинального программного продукта «*AV-OS*», разработчиком и правообладателем которого является компания «*Diebold*», с его замещением на модифицированную версию, функционал которой отличается от изначального и приводит к выдаче фальсифицированных итогов голосования. Работа электронно-вычислительной машины (ЭВМ) в соответствии с декларациями производителя и принципами избирательного права оказалась нарушена путём изменения алгоритма функционирования. В Российской Федерации применение подобного ПО является уголовно наказуемым согласно ст. 272

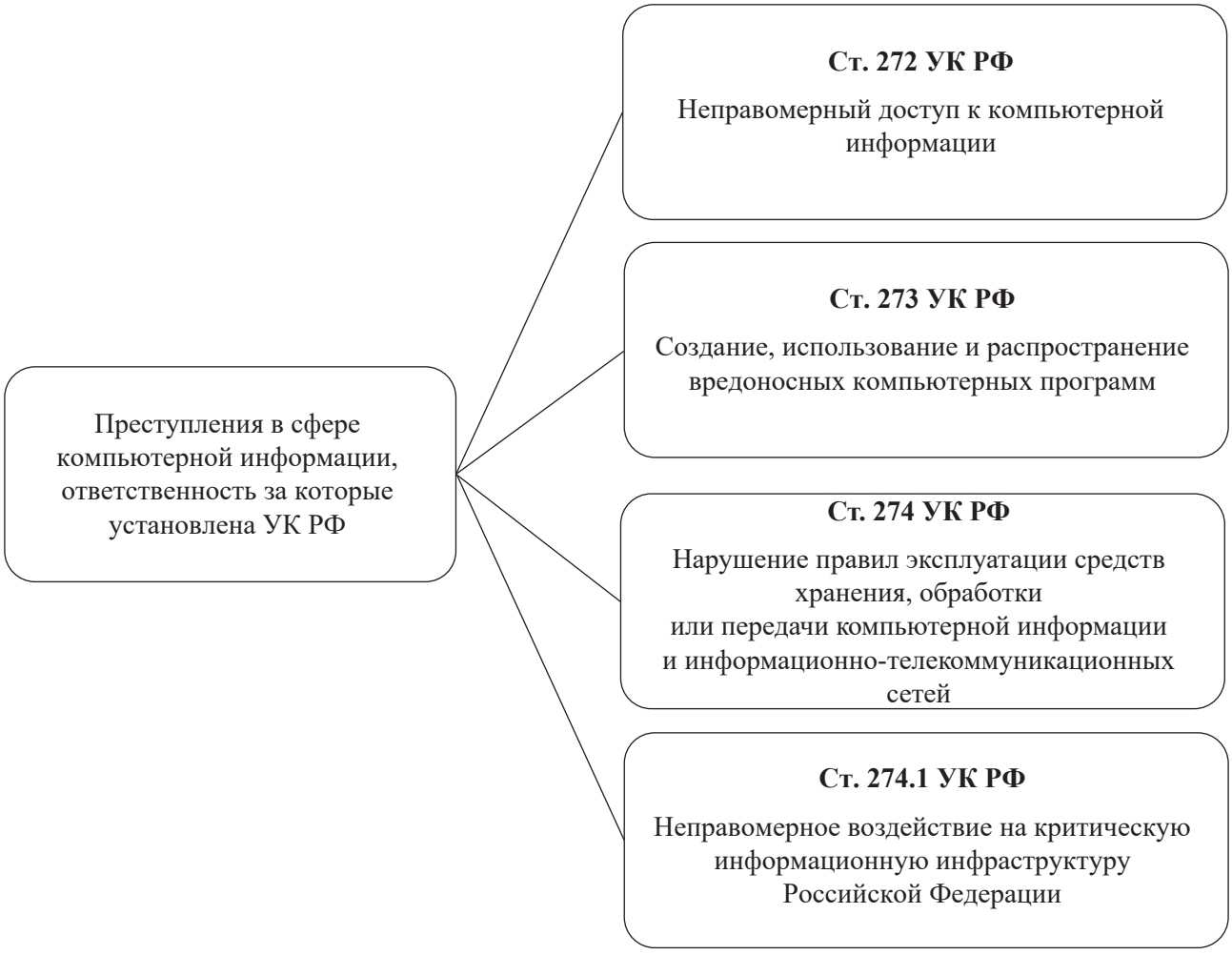


Рис. 13. Преступления в сфере компьютерной информации, ответственность за которые установлена УК РФ (составлено авторами по [12])

УК РФ (неправомерный доступ к компьютерной информации) и ст. 273 УК РФ (создание и использование вредоносных программ), а также при отнесении объекта воздействия к критической информационной инфраструктуре (КИИ) — ст. 274.1 УК РФ (неправомерное воздействие на критическую информационную инфраструктуру) [12]. Преступления в сфере компьютерной информации, обозначенные в УК РФ, представлены на рис. 13. Кроме того, установка и запуск такого модифицированного программного обеспечения в ходе реальных выборов означали бы совершение преступления, определённого ст. 142.1 УК РФ, — фальсификации итогов голосования [12].

Со стороны пользователя (избирателя, покупателя, работника и т. д.), однако, практически невозможно проверить полный реальный функционал установленного в той или иной системе ПО. Соответственно, факт фальсификации данных в информационной системе или иного вредоносного функционала (независимо от того, заложен ли он в систему тайно от общественности изначально [как это имело место в автомобилях концерна *VAG*] или внесён в неё позднее с использованием ПО, предназначенного для уничтожения, блокирования и модификации изначально заложенных алгоритмов и / или данных) с большой вероятностью может остаться незамеченным.

Схема подобного искажения данных в информационной системе представлена на рис. 14.

8. Риск биометрической фальсификации. Биометрические данные позиционируются сегодня практически как гарант безопасности. Считается, что крайне низок шанс идентичности голосовых, лицевых или дактилоскопических данных двух людей, достаточной мере для возникновения ошибки первого рода, подразумевающей принятие ложного сигнала как соответствующего критерию (ложноположительная ошибка — нулевая гипотеза об отсутствии совпадения ложно отклоняется, т. е. делается неверный вывод о совпадении с искомым лицом). Однако возникает вопрос, что можно считать крайне низким значением вероятности. При массовом внедрении биометрических систем может оказаться, что каждый или почти каждый человек будет

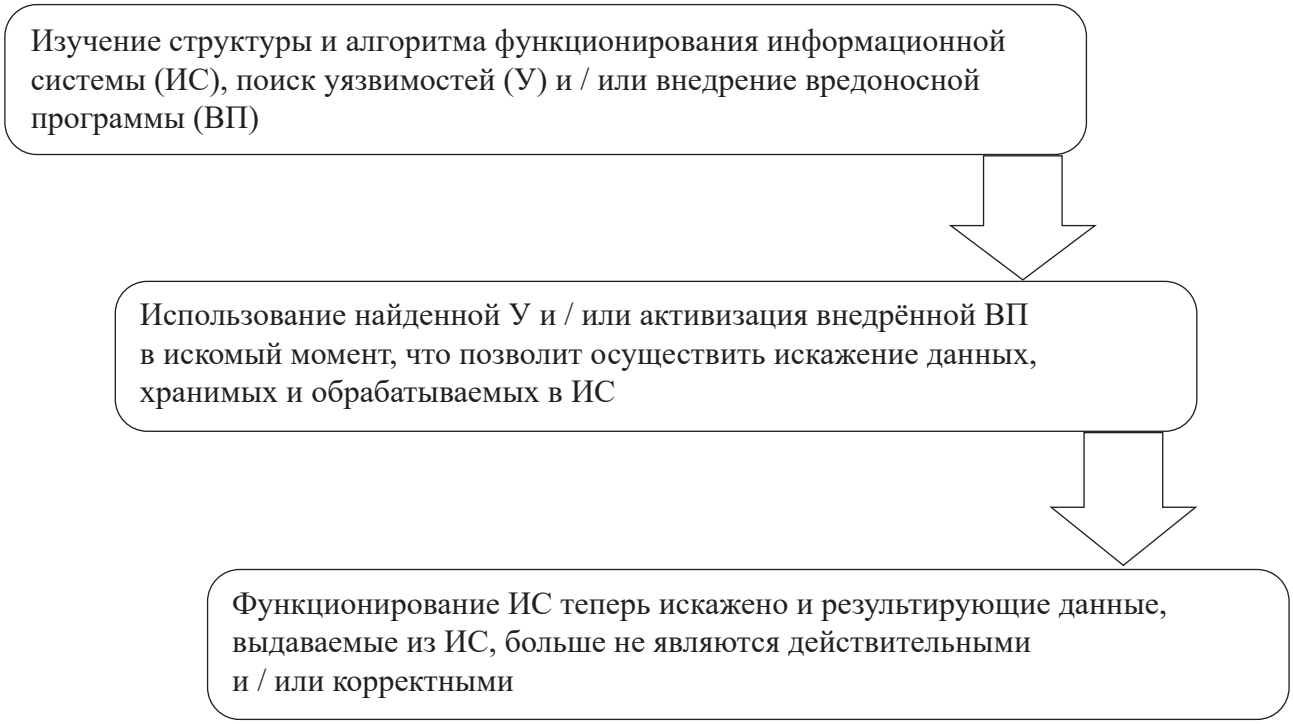


Рис. 14. Схема подмены и искажения данных, хранимых и обрабатываемых в информационной системе (составлен авторами)

подвергаться такому способу идентификации десятки раз в день, что вызовет существенный рост абсолютного числа возможных ошибок. С помощью биометрических и иных средств цифровой аутентификации сегодня предлагается совершать действия, способные нести деструктивные последствия вплоть до пожизненных: заключать кредитные договоры, оформлять продажу недвижимого имущества, производить авторизацию в системах дистанционного банковского обслуживания (ДБО). Необходимость подобных способов авторизации, на наш взгляд, представляется сомнительной для многих случаев. Аналогичной позиции придерживается и известный эксперт в области информационной безопасности, президент группы компаний «*InfoWatch*» Наталья Ивановна Касперская. Своё отношение к массовому внедрению биометрической авторизации она выразила фразой: «Зачем разменивать безопасность на потворство лени? Неужели это так сложно — пароль набрать?» [5]. Необходимо отметить, что между сделками оплаты пирожка в столовой и снятия со счёта 1 000 р. и, скажем, сделками по получению кредита и продаже недвижимости, на наш взгляд, имеется существенная разница. Если мелкие бытовые сделки совершаются регулярно и даже в случае ошибочного или несанкционированного их совершения не несут существенных рисков (вряд ли кто-то столкнулся с риском личного банкротства или существенных финансовых проблем из-за ошибочного списания оплаты проезда в трамвае или пирожка в столовой), то сделки со значительным вовлечением средств несут существенные риски. В разной степени необходимо и оперативное совершение данных сделок. Если безусловная необходимость личного одобрения в МФЦ покупки пирожка будет неприемлемой и приведёт к заметному осложнению хозяйственной деятельности общества, то для получения кредита или продажи объекта недвижимости это будет вполне разумным требованием обеспечения финансовой и информационной безопасности. Предложенная в соответствии с этим классификация сделок представлена на рис. 15.

В глобальной инфокоммуникационной сети Интернет есть видеоролик, в котором человек осуществляет эксперимент: совершает звонок в кол-центр финансовой организации (банка) и далее эмулирует с использованием специального программного обеспечения голос владельца банковского аккаунта [6]. После чего установленный в кол-центре аппаратно-программный комплекс биометрической авторизации «узнаёт» владельца и даёт доступ к банковским продуктам, соответствующим аккаунту владельца. Чтобы создать эмулированный с использованием ПО голос, достаточно было располагать аудиозаписью абсолютной любой (даже не связанной по текстовому наполнению с банковскими продуктами или требуемыми к произношению для получения доступа к ним словами) речи владельца банковского аккаунта. Далее уже специальное ПО «говорит» тем же голосом уже другие слова, которые задаются пользователем ПО (рис. 16).

Президент группы компаний «*InfoWatch*» Наталья Ивановна Касперская заявила, что средств информационной безопасности, достаточных для предотвращения злоупотреблений при работе с биометрическими данными, на сегодня просто не существует [5]. Это связано с тем, что биометрические данные, в отличие от пароля, не подлежат сколько-либо реально доступному изменению человеком в течение всей его жизни. В случае компрометации информации изменить человеку свое лицо, голос, отпечаток пальца практически невозможно. Вследствие этого требования к обеспечению безопасности хранения, обработки и использования таких данных должны быть многократно выше, чем в случае с какими-либо иными видами информации.

Таким образом, можно прийти к выводу, что внедрение современных цифровых технологий и искусственного интеллекта открывает для общества невиданные ранее возможности, но влечет весьма серьезные риски, которые особенно ярко проявляются в капиталистическом типе экономического хозяйствования.

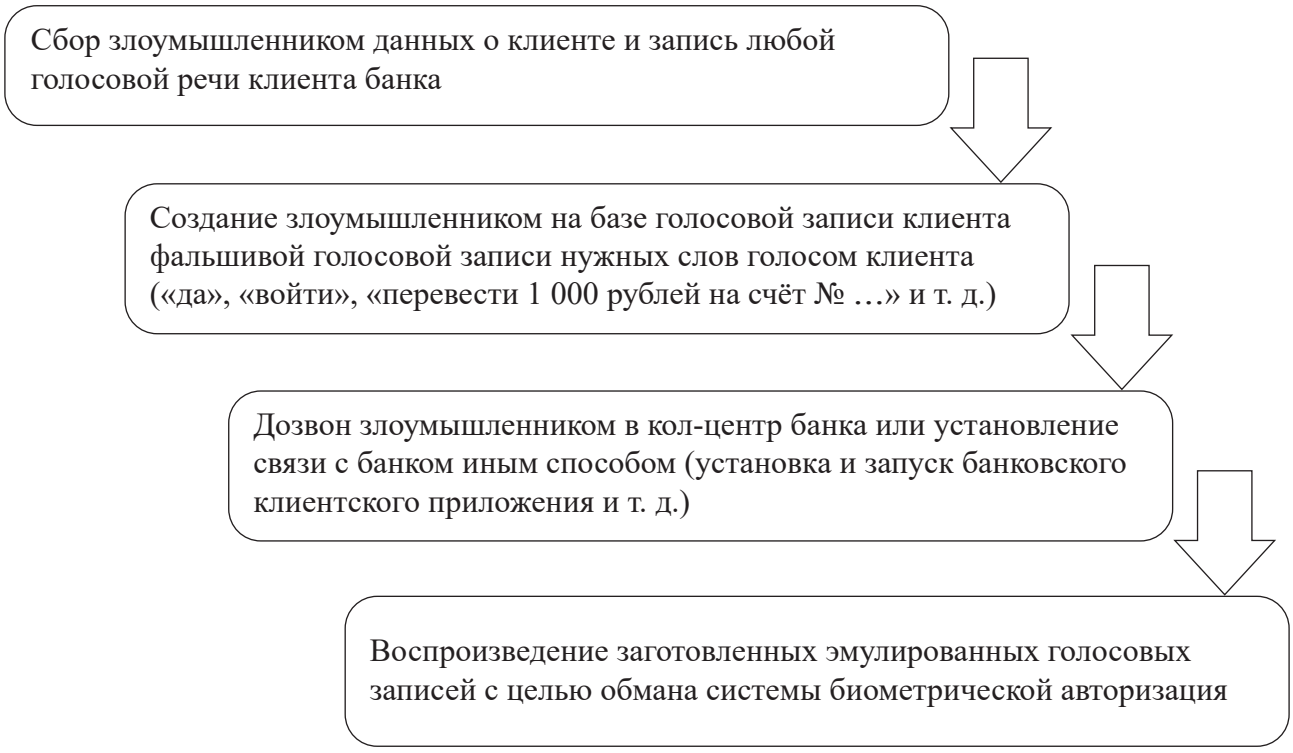


Рис. 15. Способ получения несанкционированного доступа к банковским продуктам клиента посредством фальсификации биометрических данных (составлен авторами)

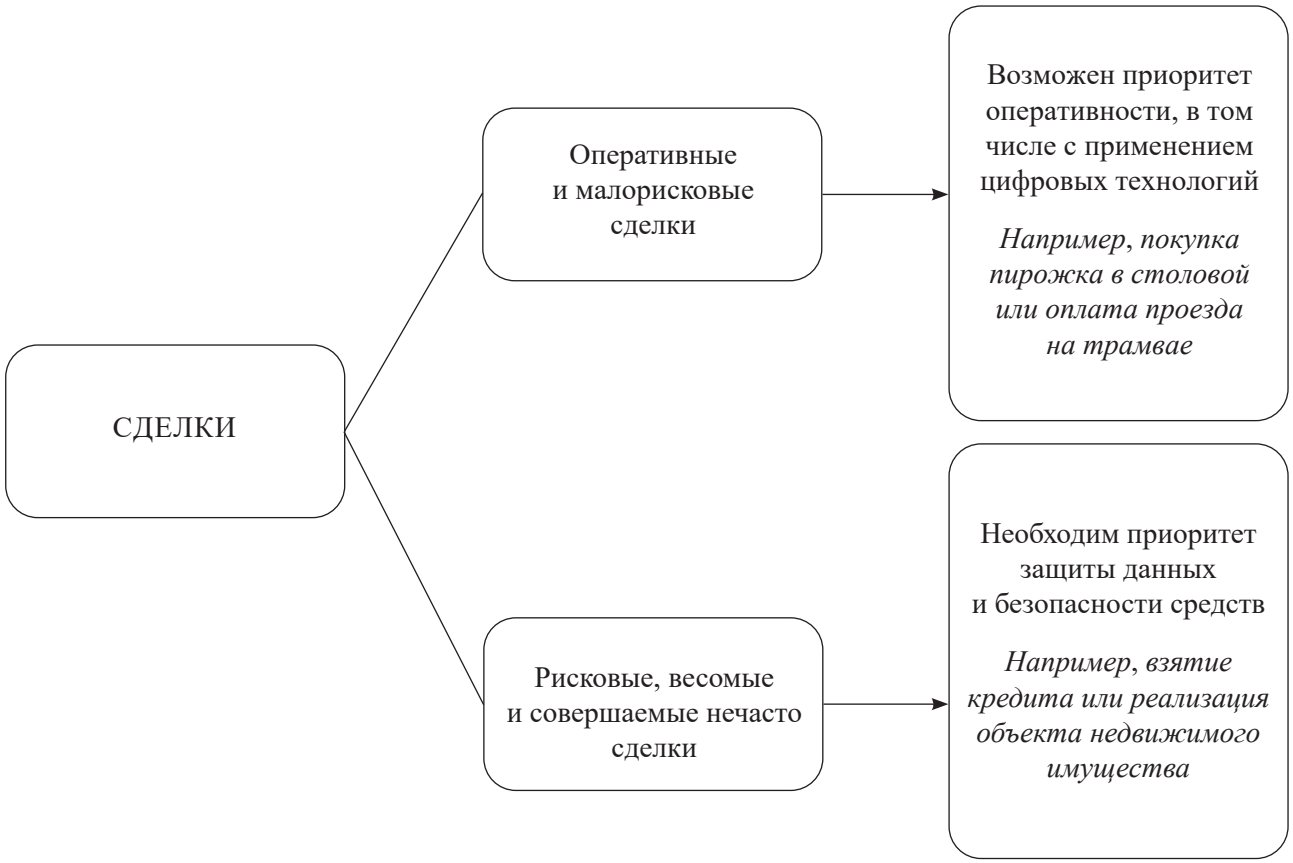


Рис. 16. Необходимые приоритеты, связанные с предложенной авторами классификацией сделок (составлен авторами)

Необходимы усиление вектора социальной направленности во избежание окончательного коллапса и так находящихся не в идеальном состоянии прав, свобод и экономических возможностей человека и реализация тщательного контроля за вероятными негативными последствиями внедрения современных информационно-вычислительных технологий для функционирования общества.

**Библиографический список**

1. Жители Сан-Франциско начали борьбу с роботакси — их обездвиживают с помощью конусов // Авто.Ру. URL: https://auto.ru/mag/article/v-sanfrancisko-opolchilis-na-robotaksi-i-pridumali-kak-ih-obezdvizhivat/.

2. Информационное общество. Федеральная служба государственной статистики РФ. URL: https://rosstat.gov.ru/statistics/infocommunity.

3. Культура и её формы // Обществознание: общество и человек. Фоксфорд: учебник. URL: https://foxford.ru/wiki/obschestvoznanie/kultura-i-ee-formy.

4. Наталья Касперская: большинство утечек в российских компаниях происходят по вине их сотрудников // Новости России. URL: https://news.myseldon.com/ru/news/index/222866070.

5. Наталья Касперская: никаких особых способов защиты биометрии нет // РИА-Новости. URL: https://ria.ru/20211006/kasperskaya-1753227872.html.

6. Нейросеть взломала биометрическую защиту в банке, используя голос владельца: посмотрите, как ей это удалось! URL: https://www.mentoday.ru/life/news/26-02-2023/neiroset-vzlomala-biometricheskuyu-zashchitu-v-banke-ispolzuya-golos-vladelca-posmotrite-kak-ei-eto-udalos/.

7. О внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 24.07.2023 № 340-ФЗ. URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=452645.

8. Об утверждении Стратегии развития электронной промышленности России на период до 2025 года: Приказ Минпромэнерго РФ от 07.08.2007 № 311. URL: https://www.consultant.ru/document/cons_doc_LAW_99457/aefc41b3c2bcefc1e715c13861b4a5e2ba165879/.

9. Проект Ермак: беспилотные КАМАЗы испытали в Арктике // АвтоРевю.ру. URL: https://autoreview.ru/articles/gruzoviki-i-avtobusy/proekt-ermak-kamazpilotniki-ispytali-v-arktike.

10. *Райзберг Б.А., Лозовский Л.Ш., Стародубцева Е.Б.* Современный экономический словарь. 6-е изд., перераб. и доп. М.: ИНФРА-М, 2023. URL: https://znanium.com/catalog/product/1904651.

11. Трампа заблокировали в соцсетях. Законно ли это? // РБК.ру. URL: https://www.rbc.ru/technology_and_media/11/01/2021/5ffc13cb9a794777cf0cbb13.

12. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 04.08.2023) (с изм. и доп., вступ. в силу с 12.10.2023) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_10699/5c337673c261a026c476d578035ce68a0ae86da0/.

13. У половины россиян нашлись деньги только на еду и одежду // Lenta.Ru. URL: https://lenta.ru/news/2019/05/28/potrebrisk/.

14. *Федотова Ю.О.* Общая биология: учеб. пособие. СПб.: Университет ИТМО, 2017. URL: https://books.ifmo.ru/file/pdf/2198.pdf.

15. Четыре промышленные революции // Постнаука.ру. URL: https://postnauka.ru/wtf/155993.

16. Электронная вычислительная машина // Современная энциклопедия. URL: https://dic.academic.ru/dic.nsf/enc1p/53550.

17. Apple начала расследование «утечки» фотографий знаменитостей из iCloud // РБК.ру. URL: https://www.rbc.ru/society/02/09/2014/570421919a794760d3d41256.

18. Apple удалила из App Store соцсеть Parler после 24-часового ультиматума // РБК.ру. URL: https://www.rbc.ru/rbcfreenews/5ffa7aa69a794717e2b2d038.

19. CPU performance. SETI@HOME. URL: https://setiathome.berkeley.edu/cpu_list.php.

20. Taking total control of voting systems: firmware manipulations on an optical scan voting terminal / S. Davtyan [et al.] // Proceedings of the 2009 ACM Symposium on Applied Computing (SAC): Conference. Honolulu, 2009. Article 2049-2053. 10.1145/1529282.1529736. URL: https://www.researchgate.net/publication/221001493_Taking_total_control_of_voting_systems_firmware_manipulations_on_an_optical_scan_voting_terminal.

21. From Apollo to Fugaku. Big Compute. URL: https://www.bigcompute.org/blog/from-apollo-to-fugaku.

22. Nigerians' Rejection of Their CBDC Is a Cautionary Tale for Other Countries. CoinDesk. URL: https://www.coindesk.com/consensus-magazine/2023/03/06/nigerians-rejection-of-their-cbdc-is-a-cautionary-tale-for-other-countries/

23. Volkswagen перепрограммирует дизельные автомобили в России // РБК.ру. URL: https://www.rbc.ru/rbcfreenews/56c3326a9a794773aff795c0.