УДК 338.26

РИСКИ МАСШТАБНОЙ ЦИФРОВИЗАЦИИ СОВРЕМЕННОГО ОБЩЕСТВА

© **Юдалевич Н. В., 2022**
Иркутский государственный университет, г. Иркутск

В данной статье рассматриваются основные риски глобальной цифровизации. Всё больше сфер жизни человека и общества переводятся в цифровой формат. В статье выявляются основные проблемы, связанные с переходом основных сфер деятельности человека в новый — цифровой формат.

Ключевые слова: цифровизация, риски цифровизации, интеллектуальная собственность, коммерческая тайна, защита персональных данных, фейковая информация, цифровое мошенничество, системный подход

Проблема стремительного развития информационных технологий (ИТ) и глобальной цифровизации, использование ИТ в повседневной жизни, давно стало предметом обсуждения, горячих споров, сомнений и неуверенности.

Под цифровизацией принято понимать внедрение цифровых технологий в различные сферы жизнедеятельности человека, в частности, и общества в целом для улучшения качества жизни, освобождения от рутины и более быстрого развития.

В современном мире всё больше и больше сфер жизни человека переходят из оффлайна в онлайн, подвергаются оцифровке персональные данные граждан, цифровизуются бизнес-процессы и пр. Новые реалии жизни подразумевают оцифровку подавляющего большинства сфер человеческой

жизни. Темпы и масштабы цифровизации растут с каждым днём.

Безусловно, цифровизация призвана улучшить жизнь человека, сделать информацию более доступной, ускорить бизнес-процессы, облегчить поиск необходимой информации, сделать более прозрачными многие операции, снизить возможность мошенничества и манипуляций, упорядочить информационные потоки и снизить потери и издержки при передаче информации.

Но, как любое явление, обладающее положительным эффектом, цифровизация сопровождается множеством рисков. В данной статье мы попытаемся рассмотреть, какие же риски глобальной цифровизации существуют на сегодняшний день.

Рис. 1. Основные риски масштабной цифровизации

Законодательная база. Хотя все риски цифровизации очень важно учитывать и по возможности минимизировать, начнем с самого, на наш взгляд, главного, с законодательной базы.

Цифровые технологии развиваются стремительно, а процедура принятия законов — дело далеко не одного дня.

«Право, как всегда, отстает от реальности и технического прогресса, а технологии заставляют нас торопиться с поиском ответа на … вопросы выработкой новых правовых решений, чтобы предусмотреть все правовые риски. Важно, чтобы в таком правовом регулировании были заложены возможные механизмы защиты интересов человека» [1].

В итоге на свет появляются, работают и участвуют в жизни человека технологии, никак или весьма слабо подкреплённые законодательством. Это касается многих сфер нашей жизни. В частности, на сегодня нет эффективных мер пресечения онлайн-мошенничества. Существует множество лазеек для совершения противоправных действий в сфере онлайн-платежей, банковского онлайн-обслуживания и многих других. Большая часть ответственности на сегодня лежит на плечах рядовых граждан — только их бдительность является гарантией, ибо не всегда возможно отличить действия официальных структур от противоправных действий мошенников.

В данном случае речь идет о том, что после совершения противоправных действий в цифровой сфере, злоумышленники просто удаляют все следы своей деятельности — сайты, банковские счета и карты, а также прочие атрибуты.

Кибермошенничество становится всё более серьезной проблемой. Мошенники используют новости как способ обмана людей в Интернете. Некоторые предлагают установить программы и другое «полезное» ПО на персональные устройства пользователей. Разумеется, не бесплатно, а за определенное вознаграждение. Подобные действия могут привести к утечке персональных данных, благодаря чему мошенники могут получить данные банковского счёта, карты и пр. пользователя, установившего ПО [6].

Правоохранительные органы не могут воздействовать на не существую на момент подачи заявления потерпевшим организацию, либо это представляется весьма затруднительным. Во всяком

случае, массово совершаемые в настоящее время мошенничества так и остаются безнаказанными.

В качестве примера можно привести поддельный сайт РЖД (существовал до февраля 2022 года) для продажи билетов на поезд, который похищал базу данных РЖД в реальном времени и якобы продавал билеты на поезд, но при оплате снимал сумму гораздо большую, чем стоимость билетов. Плательщик подтверждал оплату, не видя от кого пришел запрос и не предоставляя, разумеется, последствий. После массовых обращений потерпевших в полицию сайт исчез, но никакие суммы потерпевшим возвращены не были. Таких примеров существует масса, поддельные сайты появляются постоянно, отрабатывают некоторую сумму и исчезают, чтобы позже появиться в новом обличии с использованием быстро появляющихся новых технологий, используемых, в данном случае, во вред обществу.

В связи с таким быстрым развитием информационных технологий скорее всего необходим пересмотр процедуры и скорости принятия законопроектов в сфере цифровизации, дабы увязать скорость развития ИТ с законодательной базой, их сопровождающей и обеспечивающей их нормальное функционирование.

Далее, интеллектуальная собственность и коммерческая тайна. Разумеется, существует закон об интеллектуальной собственности, но многообразие форм последней, появляющиеся всё новые и новые ее формы, создают трудности в интерпретации закона и сложности в его исполнении.

По утверждению Всемирной организации интеллектуальной собственности «в качестве коммерческой тайны может охраняться любая информация, которая дает предприятию конкурентное преимущество и является секретной» [2]. То есть, любые методики, ноу-хау, технологии производства, инструкции по созданию или разработке и другие подобные формы являются предметом интеллектуальной собственности. Коммерческой тайной, в целом, могут являться любые сведения, дающие конкурентное преимущество организации или физическому лицу. Но как раз по причине многообразия форм интеллектуальной собственности и сведений, составляющих коммерческую тайну, весьма затруднительно формализовать, а значит и цифровизовать законодательную базу в их. В следствие чего в настоящее время наблюдается большое количество злоупотреблений в данной области. В сети Интернет часто можно найти не санкционировано размещенную информацию. Например, очень часто на пиратских сайтах можно найти литературу, продаваемую в издательствах в электронном виде. И данный вопрос на сегодня практический никак не регулируется, а явление носит массовый характер.

Далее рассмотрим вопрос защиты персональных данных. Сегодня ни одна онлайн покупка, не обходится без регистрации, при которой покупатель вынужден ввести свои контактные данные. То же касается любых других регистраций в любых цифровых сервисах, будь то обучение, оплата счетов, участие в мероприятиях и т. п. Разумеется, это необходимо для коммуникаций с пользователями, для их идентификации, для осуществления контроля и исполнения законов.

Реализация мер по защите персональных данных в соответствии с Федеральным законом № 152–ФЗ от 27.07.2006 «О персональных данных» — это зона ответственности оператора, т. е. субъекта, осуществляющего сбор и обработку данных в информационной системе. Как правило, таким субъектом выступает компания, владеющая базами данных своих сотрудников и клиентов либо сторонняя организация, уполномоченная компанией-владельцем [5]. Но при этом существуют неблагонадёжные компании, «сливающие» базы данных с персональными данными сторонним организациям, а также хищения баз данных сторонними организациями для совершения мошеннических действий.

Здесь очень важным представляется задача создания эффективных технических средств защиты персональных данных, а также обеспечить законодательную базу для эффективной борьбы с хищениями и «сливами» персональных данных в соответствии с законом об их неприкосновенности.

Также необходимо четкое правовое регулирование всех цифровых бизнес-процессов в соответствии с появляющимися и модернизирующимися постоянно цифровыми сервисами, обеспечивающими бизнес-процессы.

Подделка информации и фейки

Технологии достигли на сегодняшний день такого уровня, что подделать возможно всё: видео- и фото-контент, сканы паспортов, водительских прав, счетов, справок и т.д. Для этого используются различные программы работы с графикой — от привычного всем Adobe Photoshop’а до специально разработанных для подделки документов программ. Возможность подделки документов возрастает в разы по сравнению с доцифровым миром, она становится доступна всё более широкому кругу лиц и перестает быть чем-то недоступным [7]. Возникает целая индустрия подделки документов, своего рода теневой рынок, на котором предлагаются услуги по подделке любого типа документов.

Как избежать возможности подделки личных данных и документов? Существует рекомендация — не делиться сегодня своими данными в сети. Но на деле это представляется нереальным. Многие функции перенесены в цифровую сферу — платежи, оформление документов, покупка билетов и прочее. Как отличить, каким сервисам можно доверять персональные данные и документы, а каким нельзя и как быть уверенными в защищенности каналов, по которым передается информация от конечного

пользователя в «проверенные» организации? На сегодняшний день таких гарантий нет. Всегда есть возможность взлома, кибератаки, другого способа хищения данных. Разумеется, взломы и хищения случаются и в оффлайне. Но оффлайн общество существует неизмеримо дольше онлайн общества и в нём уже выработаны эффективные методы борьбы и механизмы пресечения мошенничества. Соответственно, он встречается, но реже, чем в онлайне.

Как же обычному члену цифрового общества уберечься от мошенничества? Пока что просто стараться соблюдать «правила гигиены» в онлайне. Без необходимости не делиться персональными данными, не отправлять документы в непроверенные источники, не знакомиться с неизвестными людьми в сети с целью проведения финансовых операций и других подобных действий, использовать только защищённые каналы связи. Также обращаться осторожно со своими паролями, хранить их в надёжном месте. Звучит как нечто совсем очевидное и, тем не менее, это самый эффективный способ не попасть в лапы цифровых мошенников.

Фейковая информация. С переходом в цифровую сферу возрастает возможность подделки не только документов, но и любой другой информации, любых фактов жизни человека и общества. Технологии находятся на таком уровне, что обычному человеку абсолютно невозможно отличить достоверную информацию от поддельной. Существует масса программ для создания, редактирования и монтажа фото и видео любой сложности, которые почти невозможно проверить на недостоверность.

Не так давно появился новый термин — фейк (fake — англ., подделка), который означает фальщшивые новости, поддельную информацию любого вида, будь то фото, видео или текст, распространяемые по цифровым медиа- и другим каналам (например, соцсетям).

Как распространяется фейковая информация? Ее могут распространять СМИИ. Как умышленно, так и по невозможности установить ее недостоверность. Она может распространяться в соцсетях самими пользователями сети. Которые уж точно не имеют надежных способов ее проверки. Фейки могут публиковать боты — программы, которые создаются специально для этой цели. Также за распространение фейковых новостей нередко отвечают реальные люди, которые публикуют со своих аккаунтов заведомо неверные данные для привлечения внимания.

Для чего создаются фейки? Во-первых, для дезинформации населения в целом и конкретных групп людей в частности, с целью формирования определенного информационного фона. Во-вторых, они могут стать инструментом для выманивания денег у населения. К ним относятся звонки якобы от банков, различные ложные просьбы о помощи, например, о переводе денег на лечение заболевшего родственника. Основная задача таких фейков — вызвать у людей определенного рода эмоции, ввести в заблуждение, побудить к определённым действиям, а также к распространению фейковой новости.

Помимо вышеописанного существует еще ряд аспектов, которые необходимо учитывать, говоря о масштабной или даже глобальной цифровизации. Сам термин «глобальная» подразумевает некую систему, охватывающую все стороны и аспекты жизни человека и общества в целом. Масштабная цифровизация, как первый этап глобальной, призвана охватить большую часть сфер жизни человека и общества. Поэтому при цифровизации общества необходим системный подход, который обеспечит корректные связи между различными частями системы всеми ее участниками. Недостаточно «оцифровать» кусочек отрасли или отдельный аспект какого-либо бизнес-процесса. Необходимо создать целостную систему, включающую все аспекты деятельности. Невозможно, а точнее, весьма неэффективно, оцифровывать лишь часть бизнес-процессов, оставляя остальное в оффлайновом режиме, поскольку стыковка данных, их проверка на соответствие и последующая аналитика для определения дальнейших действий займет нерентабельное количество времени и потратит лишние ресурсы.

Разные системы и платформы. Кроме того, необходимо учитывать тот факт, что на сегодняшний день существует множество разнородных систем и платформ, передача данных между которыми невозможна либо весьма ресурсоёмка.

Процесс цифровизации сфер деятельности человека порождает новую, до ныне не существующую экосистему, в которой формируются свои законы взаимодействия между элементами. «Экосистема — основа цифровой трансформации. Она объединяет ИТ- и бизнес-функции организации: управление ИТ, работу с персоналом HR и талантами, административно-хозяйственную деятельность (АХО), бухгалтерский учет, закупки» [3]. Как в любой экосистеме, нарушение связей и информационных потоков влечёт за собой сбои, некорректные результаты и разного рода проблемы.

Как достигнуть наилучшего взаимодействия между компонентами системы и что мешает эффективному взаимодействию.

Главной проблемой при осуществлении глобальной цифровизации является многоплатформенность. На сегодня в мире (и, в частности, в России) существует огромное количество программных комплексов, СУБД, порталов от разных производителей, которые зачастую работают как «вещь в себе», то есть дают, возможно, нужный и качественный результат в рамках одной конкретной задачи и никак не стыкуются с внешним миром.

Приведем пример понятный всем обычным пользователям — онлайн-покупки среднестатистического пользователя. Человека покупает товары повседневного спроса на различных онлайн-площадках, а также оффлайн. При это использует одну или несколько банковских карт, а также наличные деньги. Если человек захочет проанализировать движение своих средств в рамках месяца, года или на протяжении более долгосрочного периода, ему придется использовать дополнительное приложение, как минимум Excel, куда придется вбивать данные вручную. Если бы система продаж была единой экосистемой с возможностью мгновенной, а главное, автоматической системой фиксации и хранения данных о покупках, пользователь мог бы анализировать свои траты и выстраивать их более эффективным образом, отслеживая все финансовые потоки.

Что работает «на кухне», работает и в экономике в целом. Те же проблемы возникают на любом предприятии, когда информация из одной подсистемы недоступна в другой. Но то, что может делать вручную частное лицо (хоть и с дополнительными затратами) невозможно на предприятии в силу больших информационных потоков.

Итак, «единая платформа решает большинство проблем, препятствующих цифровизации компании: технологическую разрозненность систем управления, отсутствие информации по ИТ-мощностям, сложные интеграции различных сервисов, неоправданные издержки на внедрение и поддержку процессов» [3].

Следующей проблемой, достойной рассмотрения является ввод неактуальных или некорректных данных.

По данным исследования «Качество корпоративных данных 2016» неправильное применение данных может привести к финансовым потерям (как считают 42 % респондентов) и принятию неверных решений (39 %). 94 % признают, что некачественные данные вредят бизнесу, но только 40 % уверены в достоверности своих корпоративных данных. 70 % компаний уверены, что объемы данных увеличатся на 20 % в следующем году. А когда данных слишком много, они становятся проблемой. Неактуальные данные выливаются в расходы на выделение необходимой информации из моря случайных фактов [4].

Известно, что в настоящее время данные в автоматизированные системы и базы данных до сих пор вводят в основном люди, для улучшения жизни которых и осуществляется цифровизация. Пока еще существует слишком мало систем, которые сами «снимают показания» и загружают их в систему без участия человека. Человек же не застрахован от ошибок при самостоятельном вводе данных в автоматизированные системы. В итоге в системах появляется некорректная информация, которая негативно влияет на функционирование системы и выработку достоверных результатов, анализа и последующего планирования.

Говоря о многополатформенности и разнородности существующих систем, следует обратить внимание и на такую проблему, как зависимость от зарубежного программного обеспечения. Существуют признанные в мире производители того или иного ПО, утрата доступа к которому может весьма негативно сказаться на успешности работы того или иного предприятия. С другой стороны, программное обеспечение, разработанное самим предприятием, может не стыковаться с ПО и данными других разработчиков. Необходим компромисс, построенный на сотрудничестве и открытости, достижение которых пока еще весьма проблематично.

Подводя итоги, можно констатировать, что при проведении масштабной цифровизации и массовом внедрении цифровых технологий в жизнь человека в частности и общества в целом, необходимо обеспечить системный подход к процессу внедрения, а также учитывать все возможные риски. ■

1. Сазонова М. Право в цифре: какие разработки есть уже сейчас? [Электронный ресурс] // Гарант.ру: информационно-правовой портал. – Электрон. дан. – URL:https://www.garant.ru/article/1554367/?ysclid=l7y59fn0g7614875644#2 (Дата обращения: 28.09.2022)
2. Коммерческие тайны [Электронный ресурс] // WIPO: всемирная организация интеллектуальной собственности: официальный сайт. – Электрон. дан. – URL:https://www.wipo.int/tradesecrets/ru/ (Дата обращения: 28.09.2022)
3. Платформы и экосистемы [Электронный ресурс] // IT World: официальный сайт. – Электрон. дан. – URL:https://it--world-ru.turbopages.org/turbo/it-world.ru/s/cionews/business/181317.html (Дата обращения: 28.09.2022)
4. Как данные могут навредить бизнесу [Электронный ресурс] // CnewsКлуб: блоги экспертов и ИТ-компаний: официальный сайт. – Электрон. дан. – URL:https://club.cnews.ru/blogs/entry/import_kak_dannye_mogut_navredit_biznesu_d7de?ysclid=l7y5quqt4a435860722 (Дата обращения: 28.09.2022)
5. Создание системы защиты персональных данных [Электронный ресурс] // Trafic inspector next generation: официальный сайт. – Электрон. дан. – URL:https://www.smart-soft.ru/blog/praktika-sozdanie-sistemy-zaschity-personaljnyh-dannyh/ (Дата обращения: 28.09.2022)
6. Шейкин А.Г. Цифровое мошенничество: как в эпоху цифровизации злоумышленники пользуются уходом иностранного ПО с российского рынка и создают новые схемы кибермошенничества [Электронный ресурс] // Совет федерации федерального собрания РФ: официальный сайт. – Электрон. дан. – URL:http://council.gov.ru/services/discussions/blogs/134243/ (Дата обращения: 28.09.2022)
7. Цифровое мошенничество: риски и ущерб [Электронный ресурс] // Банковское обозрение: финансовая сфера: официальный сайт. – Электрон. дан. – URL:https://bosfera.ru/bo/cifrovoe-moshennichestvo-riski-i-ushcherb?amp (Дата обращения: 28.09.2022)

СПИСОК ЛИТЕРАТРУРЫ:

Как данные могут навредить бизнесу [Электронный ресурс] // CnewsКлуб: блоги экспертов и ИТ-компаний: официальный сайт. – Электрон. дан. – URL:https://club.cnews.ru/blogs/entry/import_kak_dannye_mogut_navredit_biznesu_d7de?ysclid=l7y5quqt4a435860722 (Дата обращения: 28.09.2022)

Коммерческие тайны [Электронный ресурс] // WIPO: всемирная организация интеллектуальной собственности: официальный сайт. – Электрон. дан. – URL:https://www.wipo.int/tradesecrets/ru/ (Дата обращения: 28.09.2022)

Платформы и экосистемы [Электронный ресурс] // IT World: официальный сайт. – Электрон. дан. – URL:https://it--world-ru.turbopages.org/turbo/it-world.ru/s/cionews/business/181317.html (Дата обращения: 28.09.2022)

Сазонова М. Право в цифре: какие разработки есть уже сейчас? [Электронный ресурс] // Гарант.ру: информационно-правовой портал. – Электрон. дан. – URL:https://www.garant.ru/article/1554367/?ysclid=l7y59fn0g7614875644#2 (Дата обращения: 28.09.2022)

Создание системы защиты персональных данных [Электронный ресурс] // Trafic inspector next generation: официальный сайт. – Электрон. дан. – URL:https://www.smart-soft.ru/blog/praktika-sozdanie-sistemy-zaschity-personaljnyh-dannyh/ (Дата обращения: 28.09.2022)

Цифровое мошенничество: риски и ущерб [Электронный ресурс] // Банковское обозрение: финансовая сфера: официальный сайт. – Электрон. дан. – URL:https://bosfera.ru/bo/cifrovoe-moshennichestvo-riski-i-ushcherb?amp (Дата обращения: 28.09.2022)

Шейкин А.Г. Цифровое мошенничество: как в эпоху цифровизации злоумышленники пользуются уходом иностранного ПО с российского рынка и создают новые схемы кибермошенничества [Электронный ресурс] // Совет федерации федерального собрания РФ: официальный сайт. – Электрон. дан. – URL:http://council.gov.ru/services/discussions/blogs/134243/ (Дата обращения: 28.09.2022)

Risks of global digitalization of modern society

© Iudalevich N., 2022

This article discusses the main risks of global digitalization. More and more spheres of human life and society are being transferred to digital format. The article identifies the main problems associated with the transition of the main areas of human activity to a new — digital format.

Keywords: digitalization, digitalization risks, intellectual property, trade secret, personal data protection, fake information, digital fraud, systematic approach