## Раздел 3. ЦИФРОВЫЕ ТЕХНОЛОГИИ ГЛОБАЛЬНЫХ ЭКОСИСТЕМ

### 3.1 Шифры и вирусы: защита бизнеса от внешних угроз

Ключевым для **этой сферы** цифровой экономики является понятие **конкуренции**. Риски и угрозы, которые создает в этой сфере распространение информационных технологий, следует взвешивать и оценивать именно в том контексте, как эти технологии воздействуют на **свободу конкуренции**: компаний между собой; компаний и потребителей; компаний и поставщиков, компаний, граждан и государственных органов; даже конкуренция внутри самого государственного сектора: между госорганами разного уровня, между госорганами и госкорпорациями, между регионами и т.д.

При этом становится очевидным, что само по себе только распространение информационных технологий надежного обеспечения свободы конкуренции для всех субъектов бизнеса вовсе не гарантирует.

В настоящее время, с учетом фактора стремительного развития цифровой экономики – по мере применения современных инновационных технологий, новых каналов связи, телекоммуникации и т.д. – стала меняться **концепция современного бизнеса**: от простого технологического обеспечения бизнес-процессов в сторону применения комплексных информационных систем. Именно из-за этого в современном производстве имеет место постоянная и непрерывная трансформация технологий и методов управления.

При этом новые перспективы расширяют условия для роста новых рисков, которые не поддаются количественной оценке, характеризуются отсутствием достоверной информации о связях между причинами возникновения рисков и наступлением неблагоприятных последствий. Особенно отметим наличие потенциальных (гипотетических) рисков, которые практически не рассчитываются и часто вообще не анализируются из-за отсутствия задела научных знаний в соответствующей области или виде деятельности.

Рост цифровой экономики вызывает значительные риски, связанные в первую очередь с **интернет-угрозами**. Стремительный

рост количества киберпреступлений в совокупности с утечкой информации наносит значительный ущерб, что приводит производителей к необходимости инвестирования в информационную безопасность. Имеет место отвлечение финансовых ресурсов из основной деятельности производителя. Специалистами оценивается размер ущерба только от одного инцидента информационной безопасности в размере от 1,6 млн руб. (для сектора малого и среднего бизнеса) до 11 млн (для крупных отечественных корпораций.

Бизнес постоянно сталкивается с проблемой нехватки специалистов по информационной безопасности. Значительные потери бизнеса последних лет связаны с распространением «программ-вымогателей», проникающих в компьютер и шифрующих важную информацию, с тем чтобы в последствии требовать выкуп за ее восстановление.

Некоторые угрозы, порождаемые цифровой экономикой, затрагивают также развитие рынка труда и связаны с **проблемой высвобождения больших масс работников** традиционных профессий. Повсеместная автоматизация производственных процессов в совокупности со стандартизацией базовых операций позволяет успешно заменять труд работников робототехникой, что приводит впоследствии к существенному высвобождению работников ряда специальностей, таких как кассиры, операционисты, делопроизводители, кладовщики, фасовщики, бухгалтеры начального уровня.

К примеру, в последнее время активно осуществляется процесс роботизации Сбербанком, который планирует в ближайшее время охватить до 100 своих центров. В настоящее время ряд технических задач, выполняется роботами, к примеру, решение о выдаче кредитов физическим лицам.

Процессы высвобождения низкоквалифицированных работников характерны для отечественной экономики. Согласно данным некоторых министерств и ведомств, в 2018 г. было ликвидировано 174 тыс. рабочих мест в финансовой сфере и 364 тыс. рабочих мест в торговле, автосервисе и сфере бытового ремонта.

Влияние цифровой экономики на рынок труда отражается не только в процессе высвобождения работников, но проявляется и в

**снижении величины вознаграждения низкоквалифицированных работников**. Так, с 2018 г. идет падение на 5% зарплатного предложения для низкоквалифицированных работников. Далеки от радужных прогнозы, представленные специалистами Бостонской консалтинговой группы (БКГ) относительно будущего развития рынка труда. Специалисты БКГ считают, что в ближайшие 10-20 лет в результате цифровой революции в мире исчезнет 50% профессий[8].

Анализ показывает, что Россия сегодня находится в пограничном состоянии: ряд факторов новой эпохи уже оказывает влияние на нее и ее дальнейшее развитие.

Старый уклад экономической сферы общества на данном этапе активно вытесняется таким новым направлением, как цифровая экономика. Цифровая экономика охватывает все сферы общества и активно вовлекает как физических, так и юридических лиц. Происходящие изменения в сфере экономики способствуют трансформации и других сфер жизни общества. Появляются **новые профессии и рабочие места**, которые требуют приобретения соответствующих знаний и навыков.

Важной задачей в процессе формирования цифровой экономики является **обеспечение *информационной безопасности***. При этом экономика выступает одной из сфер, где информация является важным ресурсом. Цифровая модель экономики повышает степень уязвимости информации.

*Информационная безопасность (*англ. Information Security, а также – англ. InfoSec) – практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации. Это универсальное понятие применяется вне зависимости от формы, которую могут принимать данные (электронная или, например, физическая). Основная задача информационной безопасности – сбалансированная защита конфиденциальности, целостности и доступности данных с учетом целесообразности применения и без какого-либо ущерба производительности организации.

[8] Колодняя Г. Цифровая экономика: особенности развития в России // Экономист, 2018, № 4.

Одна из ключевых проблем связана непосредственно с процессом цифровизации экономики – это **недостаточное совершенство и постоянная необходимость обновления законодательной базы**, что приводит к возникновению спорных моментов.

Существующие нормативно-правовые акты не в полной мере соответствуют реальной ситуации и остро встает вопрос защиты экономической информации, а, как известно, именно потеря экономической информации может нанести существенный вред государственной безопасности. Использование информационных технологий происходит благодаря развитию цифровой экономики, что качественно и количественно увеличивает возможности реализации всех операций посредством использования компьютера. Следует отметить, что кроме положительных моментов подобная цифровая трансформация сопровождается и определенными рисками.

Связано это с тем, что часть информации, которая принадлежит потребителям данных информационных услуг как физическим, так и юридическим лицам, носит конфиденциальный характер и подвержена таким угрозам, как ее потеря или доступ к ней иных физических и юридических лиц.

В данных условиях глобальные масштабы обретает вопрос **защиты персональных данных**. Личная информация становится одним из ценнейших активов. Наблюдается рост случаев утечки информации.

В целях решения проблемы утечки информации необходимо выявить факторы, которые способствуют потере информации. Внешние атаки обусловили 10 из 20 зафиксированных мега утечек (свыше 10 млн персональных данных (ПДн) на каждую), на которые пришлись 7,68 млрд скомпрометированных записей (98 % от общего числа). В 43 случаях объем скомпрометированных данных превысил 1 млн записей. В 53 % случаев виновными в утечках оказались сотрудники компаний, в 2 % – случаев высшие руководители и иные привилегированные пользователи.

Известно, что недостоверность или замена некоторой информации может нанести серьезный материальный и моральный вред. В данных условиях крайне актуален вопрос **обеспечения информационной безопасности государственных структур,**

**персональных данных и информации, принадлежащей коммерческим структурам**.

Прежде всего, информационная безопасность в России является зрелой и вполне успешной отраслью экономики, понимающей не только свои задачи, но и методы их решения.

Многие экономисты, аналитики и специалисты в сфере информационных технологий утверждают, что Российская Федерация должна стать в данной ситуации лидером в сфере развития цифровой экономики. Модель цифровой экономики, на основе которой строится цифровая экономика в большинстве стран, является преимущественно американской. В Российской Федерации разрабатывается и предлагается отечественный вариант цифровой экономики.

Следует отметить, что на сегодняшний день Российская Федерация является мировым лидером по объему торгов, совершенных в формате B2B и B2G. По данным статистики за 2018 г. в денежном эквиваленте он составил более 700 млрд долларов США. Это приблизительно 1,2 млн поставщиков и заказчиков. Почти все сделки осуществляются в электронном виде. Наряду с этим Россия поступательно наращивает обороты трансграничной электронной торговли, особенно после подключения к данному процессу Белоруссии и Казахстана. В частности, в рамках Таможенного союза в 2019 году объем торгов, совершенных в электронной форме в денежном эквиваленте достиг более 900 млрд долл. США. В ближайшей перспективе будет преодолена планка в один триллион долларов США.

Следует отметить, что ряд ведущих экспертов определяет электронную торговлю в качестве главного драйвера для развития цифровой экономики.

Одной из ключевых проблем в системе обеспечения информационной безопасности в условиях цифровой экономики является и **низкий уровень культуры информационной безопасности**. Работники не всегда осознают риски потери экономической информации. Кроме того следует отметить, что наибольший процент утечки приходится именно на внутренних сотрудников.

В целях формирования культуры информационной безопасности в современных компаниях необходимо регулярно проводить тренинги и семинары по повышению осведомленности работников, а корпоративные службы информационной безопасности (ИБ) должны быть максимально открыты для взаимодействия с коллегами из других подразделений при возникновении вопросов и проблемных ситуаций.

Таким образом, информационная безопасность становится сегодня важнейшим фактором развития цифровой экономики, расширения электронного взаимодействия участников рынка, внедрение элементов блокчейна. Масштабное использование новых технологий выводит на первый план вопросы повышения конкурентоспособности отечественной финансовой системы, обеспечение ее безопасности как объекта критической информационной инфраструктуры. Защищенность информационных систем имеет для страны стратегическое значение. Вместе с тем ситуация явно обостряется с ростом уровня угроз в информационном пространстве, при этом методы, способы и средства таких преступлений закономерно становятся все сложнее, что требует адекватных мер по повышению киберустойчивости субъектов финансового рынка.

В качестве одного из инструментов защиты экономической информации выступает ***криптография***. Технологии криптографии позволяют реализовать следующие процессы информационной защиты:

- идентификацию объекта или субъекта сети или информационной системы;
- аутентификацию объекта или субъекта сети;
- контроль/разграничение доступа к ресурсам локальной сети или внесетевым сервисам;
- обеспечение и контроль целостности данных.

При этом переход на российское шифровальное программное обеспечение с учетом огромного опыта является одним из ключевых инструментов защиты информации в современном экономическом пространстве России.

Криптография (от др.-греч. κρυπτός «скрытый» + γράφω «пишу») – наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним), целостности данных (невозможности незаметного изменения информации), аутентификации (проверки подлинности авторства или иных свойств объекта).

Программа «Цифровая экономика», в рамках которой предусмотрен переход на отечественное шифровальное программное обеспечение является хорошим фундаментом. Осуществить полный переход участников процесса обмена цифровой информацией в рамках системы «Цифровая экономика» на российские системы шифрования данных разработчики планируют к 2021 г. В рамках данного проекта необходимо встроить российские программы шифрования в программное обеспечение.

В мире на данный момент функционируют **две школы шифрования**: Россия и США. Китай также начал активно заниматься данным вопросом. При этом российские алгоритмы вполне надежны. Российские алгоритмы одобрены специальным комитетом Международной организации по стандартизации (ISO). Со стороны крупнейших мировых IT-корпораций наблюдается настороженность и отказ от их использования, несмотря на признание Международной организацией по стандартизации.

На данный момент шифрование данных осуществляется по американским сертификатам безопасности. В этой ситуации российские пользователи оказываются под угрозой рассекречивания своих данных, которые хранятся на различных сайтах, в случае отзыва этих сертификатов их владельцами.

В свете существующей ситуации в сфере информационной безопасности отмечается также еще один факт, представляющий опасность для российских пользователей сети и указанный в проекте программы. По многим оценкам примерно 60 % информации, передающейся как бы внутри российского информационного пространства, проходит, тем не менее, через серверы других государств, что значительно повышает риски.

Для поддержания режима информационной безопасности особенно важны **программно-технические меры и средства**,

поскольку основная угроза компьютерным системам находится в них: сбои оборудования, ошибки программного обеспечения, промахи пользователей и администраторов и т.п.

Необходимо также и формирование **правового фундамента для обеспечения информационной безопасности в кредитно-финансовой сфере**, первым делом сославшись на программу «Цифровая экономика Российской Федерации», утвержденную распоряжением правительства России от 28 июля 2017 г., одним из направлений которой определена необходимость нейтрализации рисков, связанных с киберустойчивостью финансовых организаций. Важным документом является положение Доктрины информационной безопасности России, принятой указом Президента в декабре 2016 г.

Значимым событием для отрасли в 2017 г. стало вступление в силу закона «О безопасности критической информационной инфраструктуры РФ». Показатели критериев значимости для них будут установлены постановлением Правительства. Предполагается, что в их основу ляжет среднедневное количество операций, осуществляемых субъектом отечественной информационной инфраструктуры. В соответствии с данным показателем к значимым объектам критической информационной инфраструктуры третьей категории в кредитно-финансовой сфере могут быть отнесены информационные и автоматизированные системы Банка России, Сбербанка, Национальной системы платежных карт, других значимых кредитных и финансовых организаций.

Важной функцией регулятора становится содействие в предоставлении данных в государственную систему обнаружения, предупреждение и ликвидация последствий компьютерных атак на информационные ресурсы России.

Банком России создан специализированный Департамент информационной безопасности. На 2018 г. основная задача центра компетенций регулятора по обеспечению киберустойчивости организаций кредитно-финансовой сферы – это активизация информационного обмена о прецедентах с финансовыми организациями.

Кроме того, новый департамент будет определять потребности рынка в совершенствовании системы киберустойчивости, заниматься

нормативным регулированием, предполагается, что спектр его функций будет достаточно широк. Информационный обмен с субъектами финансового рынка будет организован по определенной технологии в установленном формате электронных сообщений.

По многочисленным заключениям аналитиков, почти 99 % всех киберпреступлений в мире связаны с воровством денег. Наибольшую опасность для банков сейчас представляют целевые атаки, ущерб от которых в прошлом году вырос почти на 300 %. Одна из атак стоила российскому банку 140 млн руб., а общая сумма хищений выросла, по оценкам экспертов, до 2,5 млрд руб.

Количество утечек информации возрастает с каждым годом, особенно в условиях формирования цифровой экономики. Так, с 2006 по 2018 г.г. количество утечек конфиденциальной информации возросло в 8 раз. Основной причиной потери конфиденциальной информации по-прежнему остаются внутренние факторы. Например, основной процент приходится на сотрудников, более половины утечек происходит именно по вине сотрудников, но следует отметить снижение данного показателя в 2018 г. по сравнению с 2017 г.

С другой стороны, использование цифровых технологий создает благоприятные информационные возможности повышения безопасности на разных уровнях.

Бездумное вхождение в мировую цифровую экономику, включение в мировые цифровые цепочки создаст особые возможности для стран, более развитых в цифровом направлении, и сделает объектом манипулирования менее развитые страны. **Особенно остро стоит проблема кибербезопасности.**

Россия обязана сохранить суверенность экономики, общественно-политической жизни и национального развития, тем более исходя из существующих ныне геополитических сложностей. Имеется и внешнеэкономическая опасность, связанная с возросшими возможностями вывоза капитала за рубеж и многочисленными экономическими санкциями.

18 декабря 2017 г. Правительственная комиссия по использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности

утвердила две программы «**Цифровая экономика Российской Федерации**» на 2018-2024 гг. По итогам реализации этих программ должны быть достигнуты целевые значения информационной безопасности на сетях связи и в российском сегменте интернета. Должна быть создана система стимулов для приобретения и использования компьютерного, серверного и телекоммуникационного оборудования российского производства. Созданы механизмы стимулирования использования отечественного программного обеспечения всеми участниками информационного взаимодействия.

Помимо этого, требуются и уже в разработке национальные *стандарты киберфизических систем*. Необходимо увеличить контроль обработки и доступа к персональным данным, большим пользовательским данным, в том числе в социальных сетях и прочих средствах социальной коммуникации.

*Киберфизические системы (Cyber-Physical System, CPS)* – это системы, состоящие из различных природных объектов, искусственных подсистем и управляющих контроллеров, позволяющих представить такое образование как единое целое. В CPS обеспечивается тесная связь и координация между вычислительными и физическими ресурсами. Компьютеры осуществляют мониторинг и управление физическими процессами с использованием такой петли обратной связи, где происходящее в физических системах оказывает влияние на вычисления и наоборот.

Также ожидается, что по итогам выполнения программы будет разработана система мер поддержки российских производителей продуктов и услуг информационно-компьютерных технологий, осуществляющих патентование продуктов за рубежом.

Утвержденный план содержит также перечень целевых показателей и индикаторов. С 10 % в 2018 г. до 90 % в 2024 г. должна увеличиться доля субъектов информационного взаимодействия, использующих стандарты безопасности в киберфизических системах. Доля граждан, повысивших грамотность в сфере информационной безопасности, медиапотребления и использования интернет-сервисов, к 2024 г. должна составить 50 %.

В целом же в российской экономике цифровая трансформация будет оказывать возрастающее влияние на разные отрасли. ВВП до

2025 г. согласно всем расчетам должен увеличиться от 0,4 % до 0,9 % в связи с внедрением цифровой экономики. Сравнение роста ВВП с прогнозируемыми темпами роста прогнозов российской экономики позволяет сделать вывод, что цифровизация приведет к росту ВВП с 2015 по 2025 гг. от 19 % до 34 %.

В настоящее время это самая актуальная тема для развития любой страны. Цифровая экономика может приводить к возникновению «умных» городов, транспорта и сельского хозяйства, отсутствию цифрового неравенства отдельных регионов, повышению цифровой грамотности у населения.

Также человечество может столкнуться и с **отрицательными сторонами данной сферы**: нарушение безопасности конфиденциальности личных данных населения, засорение информационного пространства, дефицит высокообразованных кадров и, наоборот, появление большого количества безработных людей, которые появились в результате внедрения цифровой экономики. В данном случае преимуществ будет больше, чем недостатков, поэтому необходимо развивать данную сторону экономики и внедрять ее во всех регионах.

В частности, острой проблемой становится нехватка кадров, необходимых для развития цифровой экономики. Действительно, переход к цифровым методам хозяйствования оказался очень выгоден – обслуживание клиентов в интернете гораздо дешевле, чем обслуживание их в офисах (зарплата операторов, аренда офисов и т.п.). Но для разработки таких обслуживающих систем возник дефицит программистов.

Налицо дисбаланс спроса и предложения, и, чтобы удовлетворить спрос, веб-разработчиков стали готовить ускоренными методами, типа «стань веб-программистом за три недели», в которых нет места безопасной архитектуре и безопасной разработке. Такие разработчики стоят недорого, поэтому команды из них легко выигрывают конкурсы «кто меньше запросит за конкретный функционал». В результате качество веб-приложения год за годом падает, поскольку фокус разработчиков направлен прежде всего на функционал, а не на безопасность. То же самое относится и к инженерам, которые настраивают инфраструктуру для приложений, и к сотрудникам

информационной безопасности, которые настраивают средства защиты.

Цифровизация экономики потребует быстрого роста количества приложений, а значит – и разработчиков, тестеров, инженеров и «безопасников».

### 3.2 Цифровизация, риски и конкуренция в глобальном мире

Бизнес сегодня – достаточно динамичный процесс, требующий постоянных изменений, а поскольку бизнес будет реализован в приложениях, то такими же гибкими и постоянно меняющимися должны стать и приложения. А это требует полной перестройки подхода к цифровому бизнесу не только специализированных профессионалов, упомянутых выше, но и каждого участника процесса.

Поэтому сегодня непонятно, как можно «оцифровать» экономику, не имея армии рядовых «оцифровщиков», как из области ИТ, так и из области самого бизнеса.

Следующей, не очень явно видной на первый взгляд, но принципиальной проблемой «оцифровки» является то, что в цифровом бизнесе ИТ и бизнес как бы меняются местами. В традиционном аналоговом варианте бизнес происходит сам по себе, а ИТ является его отражением, часто с целью учета или аналитики. То есть сначала транзакции, операции, договора и т.д. происходят в аналоговом, бумажно-наличном мире, а потом (иногда очень быстро, практически мгновенно) они заносятся в ИТ-системы для учета и анализа. Если в аналоговом мире что-то происходит с ИТ-системой и данные теряются, то с бизнесом ничего особенного не произойдет, понадобится лишь время для восстановления данных из их аналоговых источников.

В цифровой экономике нет никакой «первички». Все сделки происходят в цифровом пространстве, в бизнес-приложениях, то есть теперь ИТ не отражает бизнес, а сами по себе бизнес-приложения и есть бизнес. Раньше при падении ИТ-системы нефть продолжали добывать, платежи проходили медленнее, но проходили, билеты

выписывали вручную. Теперь при падении системы наступает полный коллапс – даже сугубо аналоговые процессы перестают работать, потому что системы управления ими стали цифровыми. То есть с переходом на «цифру» даже самый аналоговый бизнес должен понять, что ИТ – это не служебная функция, а среда существования бизнеса, его ядро. Сегодня это хорошо понимают лишь интернет-гиганты и отдельные инноваторы, такие как банки без офиса. Без тотального распространения такого знания и соответствующей смены подхода к ИТ никакой цифровизации не случится.

**Значительны также риски цифровой идентификации.** Цифровая экономика подразумевает цифровые интерфейсы, а это означает и замену аналоговой идентификации по принципу «прийти в офис с двумя документами» на полностью цифровую. Это настолько удобно, насколько и рискованно – возникают угрозы полноценной кражи личности, то есть гражданских и потребительских действий от имени другого человека. Дальше – больше. Есть риски цифровизации аналоговой экономики, а есть риски самой цифровизации.

Теперь приведем конкретный **пример системной работы с рисками в бизнесе** – из практики в сфере промышленного производства.

Системный подход в этой сфере определяется тем, что за исходную позицию принимается ежемесячная разработка промышленно-финансового плана предприятия. На этой основе затем формируется матрица организационной структуры предприятия.

В дальнейшем определяются требования и выбирается конкретная методика применения управленческих систем.

Далее имеет место структурирование, сегментирование, верификация и валидация отдельных этапов проекта.

После этого определяются обязанности и полномочия всех участников проекта в ходе реализации утвержденного Сценария бизнес-процесса – в строгом соответствии с паспортом рабочего места и разработанной технологической картой данного процесса.

Во многих проектах сформулирована обязанность всех участников принимать содействие в реализации Сценария бизнес-процесса в строгом соответствии с паспортами их рабочих мест и с разработанными для них технологическими картами данного процесса.

При этом непременным ограничением всегда является утвержденный жесткий бюджет финансового планирования проекта. Особенностями организации работы по проекту в данном случае применение двухканальной системы управления предприятием, а также полная и комплексная диспетчеризация всех бизнес-процессов через единый диспетчерский центр, дублирование, резервирование, систематизирование и контроллинг всех текущих управленческих действий и дублирование, кворумирование, верификация и валидация всех этапов проекта службой экономической и информационной безопасности предприятия.

Одновременно осуществляется также системная подготовка кадров на собственной учебной базе предприятия.

И в основе всей этой работы действует механизм сбора статистической информации о KPIs каждого участника бизнес-процесса через глобальную информационную сеть предприятия.

Следующим направлением было выявление и оценка логистических рисков в деятельности предприятия, а именно: определение конкретных рисков материально-технического обеспечения, оценка вероятности каждого риска, оценка уровня потерь, разработка мер по минимизации каждого риска и предложений по их профилактике (избежание рисков, диссипация (распределение) рисков, «торможение» рисков, передача или компенсация исков).

Для целей избежания логистических рисков применятся практика заключения договоров поставки одноименного вида сырья не менее чем с двумя поставщиками. При этом выбор поставщика сырья осуществлялся на тендерной основе. Проводился также комплексный анализ деятельности поставщика и проверка его репутации на рынке, одновременно проводился маркетинговый мониторинг соответствующего рынка. Правилом является и заключение долгосрочных и стабильных договоров на поставку сырьевых компонентов, обязательное наличие страхового запаса сырья на предприятии и поддержка отношений с потенциальными поставщиками, готовых в любой момент сменить сомнительных или недостаточно надежных поставщиков сырья.

Другими условиями профилактики логистических рисков являются: гарантийные обязательства каждого поставщика по качеству,

количеству и своевременности поставки ресурса; страхование от поставок некачественного сырья; возможность сочетания поставщиков с диаметрально противоположных рынков (например, из Бразилии и Китая); полное информационное обеспечение технологического логистического процесса поставки сырья. Оцениваются также возможности перехода на альтернативное сырье и перехода на другой ассортимент выпускаемой продукции, включая разработку аварийно-резервной ассортиментной матрицы товаров, в случае невозможности выпускать традиционный продукт, в том числе и с использованием резервной технологии.

Важной считается задача доведения качества сырья до оптимальных значений через систему полного факторного эксперимента и нейросетевые модели управления.

В этих условиях полезным может оказаться использование метода фрагментограмм. При этом под фрагментограммой следует понимать матрицу взаимосвязей проблемных условий, ситуаций (или рисков), решение которых существенно изменяет исходные параметры, так как раскрывает не только уровень оказываемого влияния на тот или иной элемент системы, но и помогает установить связи между субъектами, участвующими в рассматриваемом процессе, а именно связи между их поведением и его последствиями. Все это в конечном счете помогает оценить взаимодействия между собой отдельных элементов (фрагментов) матрицы.

Соответственно для каждого вида деятельности должны создаваться (разрабатываться) свои фрагментограммы, учитывающие специфику бизнес процессов этого вида деятельности.

При этом решение задачи прохождения фрагментов сводится к поиску первоочередных проблем, устранив которые можно существенно улучшить предсказуемость развития событий в данной области, а также снять или значительно ослабить другие риски.

Главная цель этого метода состоит в переходе от каскадных барьеров к барьерам второго уровня – с соответствующим уменьшением неопределенности при формировании бизнес-процессов. В свою очередь это приводит к более высокой вероятности наступления планируемого события, тем самым повышая устойчивость рассматриваемой информационно-производственной системы в целом.

Подводя итог, можно отметить, что России понадобится некоторое время для создания в ключевых секторах цифровой экономики конкурентоспособных предприятий. Но первый и решительный шаг в этом направлении – масштабное применение IT-технологий с учетом возникающих рисков и поиском методов их минимизации – уже сделан.

При этом анализ и оценка ряда источников научно-технической информации, а также статистических данных развития некоторых стран, отраслей и отдельных компаний показывает, что начавшийся около двух десятилетий назад переход от постиндустриального общества к обществу информационному завершается. Это выразилось, в частности, в значительном изменении экономического уклада, появлении новых факторов нестабильности, социально-политической активности населения и новых угроз безопасности.

Это будущее, которое уже явилось результатом практической реализации и внедрения целого ряда новинок в области информационных технологий. Наше настоящее – это наше вчерашнее будущее, в котором уже устойчиво закрепился смартфон, как неотъемлемая частица социального образа современного человека, и развивается принципиально новый рынок мобильного контента. Наконец, настоящее – это вчерашнее будущее, когда только еще появился феномен так называемых детей индиго. А сегодня это поколение, первое поколение, воспитанное на мобильном контенте, видеороликах с Youtube и игровых стримах как новом виде искусства, входит во взрослую жизнь, получая гражданские права избирателей.

В этом контексте общая оценка происходящих фундаментальных изменений следующая: без серьезных и кардинальных изменений в мировосприятии и международных отношениях в среднесрочной перспективе мир рискует столкнуться с дальнейшим все ускоряющимся ростом социального неравенства, появлением новых, ранее неидентифицируемых угроз личной и коллективной безопасности, стремительному дисбалансу отношений в мире в целом.

Как результат – существующая система международного контроля и управления, система издержек и противовесов не сработает и мир окажется в крайне нестабильном состоянии, когда даже малейший конфликт может спровоцировать большую войну.

В числе **угроз**, которые порождают описанные изменения, следует отметить следующие.

– **Кардинально меняется финансово-экономический уклад.** В новых условиях роста скоростей оборачивания капитала, а также изменения таких понятий, как валовой продукт, производительность труда принципиально по-иному оцениваются результаты экономического развития. К примеру, сегодня уже появились отрицательные проценты по депозитным вкладам, а налоги взимаются не по итогу отчетного периода, а по факту каждой транзакции. На этом фоне существующие и применяемые методики статистического учета и прогнозирования остаются прежними, что ведет к возникновению опасного дисбаланса в оценке реального состояния дел в экономике. Кроме того, меняется само понятие деньги. Сегодня все шире используются так называемые криптовалюты. Принципиальное их отличие – отсутствие единого центра эмиссии. Государства утрачивают возможность эмитировать валюту и тем самым изменять ее обменный курс в зависимости от собственных предпочтений. Это также негативно сказывается на возможности государств накапливать средства в разного рода фондах, поскольку стоимость хранения средств в них возрастает достаточно быстро и они становятся обузой для экономики. Важнейшая особенность криптовалют – их сетевая структура. Этот факт ставит на повестку дня снижение значимости таких понятий, как финансовый центр, а это в свою очередь, ведет к утрате контроля со стороны мировой элиты над глобальными финансовыми потоками.

– **Наблюдается резкий рост производительности труда в новых отраслях, связанных с обработкой информации, созданием контента и программных продуктов**, что в целом ведет к резкой потере значимости человека как производящей единицы. Сегодня, к примеру, один программист может управлять сложным и мощным информационным порталом, заменяя десятки журналистов и других работников. Та же ситуация и на производстве – введение в строй мощных роботизированных производственных линий, создание полностью автоматических производств снижает потребности работодателя в персонале, существенно экономя на социальных выплатах. По ряду оценок, в ближайшие 20 лет до 50% существующих сегодня профессий утратят свое значение. Все это в совокупности ведет к возникновению серьезных проблем с занятостью населения, а дополни-

тельно – к проблеме пенсионного и медицинского обеспечения. Государства перестают справляться с основными своими обязательствами перед гражданами, а социальная нестабильность возрастает.

– **Расширяется применение мощных средств вычислительной техники и систем математического моделирования**, что резко ускоряет процессы в ряде направлений научных исследований. Так, серьезные изменения коснулись материаловедения и новых технологий производства. Появилась возможность синтеза веществ с новыми, уникальными свойствами, и создания на их основе уникальных продуктов. Завершение промышленного внедрения технологии 3D-печати кардинально меняет ситуацию в целом ряде отраслей: появляется возможность создания уникальных устройств (например, авиационных и ракетных двигателей), которые были невозможны без этой технологии. Это может принципиально повлиять, в частности, на рынок вооружений и в целом на распространение оружия (особенно, стрелкового). Сегодня нет необходимости трансграничной пересылки готовых образцов вооружения – все, что необходимо, можно распечатать на месте, достаточно просто скачать нужный файл для 3D-принтера.

– **Меняется доступность космического пространства.** Развитие отраслей материаловедения, микроэлектроники и др. позволяет сегодня создавать ракеты-носители крайне малых размеров, пригодные для выведения на околоземную орбиту компактных спутников малой массы, а достижения в микроэлектронике позволяют получить высокие показатели эффективности единицы массы, выводимой в околоземное пространство. Для таких ракет закрыты геостационарные орбитальные позиции и обитаемые корабли, но обеспечить связь и ретрансляцию, электронную разведку, решить некоторые иные задачи, микроспутникам под силу. Вместе с тем, им не нужны сложные и дорогостоящие комплексы подготовки и выведения, что существенно снижает порог вхождения в число игроков космической гонки.

– **Достижения в 3D-печати кардинально меняют возможности медицины**. Уже опробована печать собственными стволовыми клетками практически любых органов и тканей человека без их возможного последующего отторжения.

– **Переход в производстве микроэлектронных компонентов на 5-7 нм технологии** влечет за собой резкий скачок в развитии вы-

числительной техники, а вместе с ней – и всех связанных отраслей, как военного, так и гражданского назначения. Причем нынешний скачек фактически открывает принципиально новые возможности по интеграции и созданию суперкомпьютерной техники.

– **Достижения микроэлектроники дополняются достижениями в алгоритмистике и создании сложных программных комплексов**, прежде всего, в области систем искусственного интеллекта, виртуальной и дополненной реальности. Прорыв в области глубокого машинного обучения открывает принципиально новые возможности в поиске новых лекарственных форм, создании уникальных систем анализа и принятия решений.

– **Завершение расшифровки генома человека открыло возможность генетической медицины**, которая не только дает возможность устранения врожденных генетических дефектов, но и позволяет перейти к новому этапу – к созданию «абсолютного человека» – евгенике. Это одна из крайне опасных и тревожных тенденций развития человечества. Поскольку генетическая терапия достаточно дорогостоящая, она во многом доступна для богатых.

– **Развитие контента, отработка технологий виртуальной и дополненной реальности создает условия дальнейшей атомизации общества** – все больше времени человек будет проводить не в реальном, а в виртуальном мире. Это новые условия для трансформации политической системы. Уже сегодня выборы в США и во Франции показали, что основной вклад в победу тех или иных кандидатов сделали виртуальные социальные сообщества. Уже сегодня ясно, что подобно тому, как в XX веке на пике расцвета индустриального общества зародилась «Партия зеленых», в основу мотивации которых было положено не классовое неравенство, а борьба за экологичный мир, следует ожидать, что в нынешних условиях тенденция может быть схожей и появятся механизмы политической борьбы, адекватные происходящим изменениям.

– **Принципиально меняется «ландшафт» угроз безопасности личности и государства**. Расширение проникновения информационных систем в системы государственного и военного управления, в системы управления вооружением ставит высшим приоритетом угрозы информационной безопасности и защиты информации. Отдельно

следует говорить об информационном или кибертерроризме, когда даже один человек в состоянии совершить противоправное деяние, затрагивающее целые государства и даже группы государств.

– **Практически полностью утрачивается понятие конфиденциальность и частная жизнь.** Повсеместное развитие систем видеонаблюдения, баз персональной информации, систем анализа больших данных и др. делают человека фактически «прозрачным» для любого, кто располагает доступом к его персональной информации.

– **Фактически не осталось простых мобильных телефонов**. Их заменили **смартфоны**. И эти смартфоны, фактически, стали электронными аватарами своих хозяев: они находятся всегда при них, указывая текущее местоположение хозяев; они обобщают информацию о посещаемых сайтах, контактах, местах, в которых бывает их хозяин, они располагают информацией о платежах и многое другое. Доступом к большинству такой информации обладает оператор мобильной связи. Сегодня эти компании становятся новыми транснациональными компаниями информационной эпохи.

– **Особую значимость приобретают риски возможности манипулирования информацией**. Сегодня складывается ситуация, когда традиционные средства массовой информации утрачивают свое значение, более того, они становятся механизмами тиражирования ложных новостей и фактов, что фактически нивелирует их роль и значение в новом мире, и требует кардинального изменения не только самой технологии работы с новостями, но и технологии аутентификации и идентификации источников этих новостей.

– **Развитие технологий работы с большими объемами информации и стремительный рост вычислительных мощностей позволяет создавать алгоритмы оценки ситуации, работающие в реальном масштабе времени.** Это уже привело к развитию направления «Аналитика 3.0», что обусловлено созданием принципиально новых подходов к анализу информации. Сегодня, в частности, сделки на фондовых биржах совершаются за доли секунды, при этом компьютер успевает проанализировать большие объемы информации по предыдущим сделкам и определить рациональную торговую стратегию. Во многих случаях, за то время, пока пользователь переключается между соседними страницами какого-либо сайта, система успевает

проанализировать его предпочтения и сгенерировать следующую страницу, на которую он только переходит, в том виде, в каком он желал бы ее видеть.

– **Развитие средств искусственного интеллекта, передача им задач управления комплексами вооружения и военной техники,** формируют целый пласт принципиально иных задач, требующих решения – юридического и морально-этического обоснования применения оружия против человека в условиях, когда решение о применении принимает машина.

Перечисленные выше особенности текущего этапа развития современного общества являются лишь наиболее значимыми. Общее количество изменений значительно больше и их влияние на современную жизнь еще глубже.

*Глобализация и цифровизация* – два процесса, представляющие две стороны одного общего явления – интернационализации жизни стран и народов мира. Конкурирующим с ними является понятие национального интереса. Глобализация и цифровизация увязывают страны и народы в единый рынок, а национальный интерес позволяет каждой стране найти на этом рынке свое место.

*Глобализация* — процесс всемирной экономической, политической, культурной и религиозной интеграции и унификации. Глобализация является характерной чертой процессов изменения структуры мирового хозяйства, понимаемого как совокупность национальных хозяйств, связанных друг с другом системой международного разделения труда, экономических и политических отношений, путем включения в мировой рынок и тесного переплетения экономики на основе транснационализации и регионализации.

Особенность процесса глобализации состоит в том, что сильные страны от него крепнут и богатеют, а слабые получают шанс на догоняющее развитие. Но – только шанс, если страна не может или не желает использовать этот шанс, то глобализация, наоборот, все более заталкивает ее в пучину бедности и отставания.

У глобализации и цифровизации есть еще одна **общая черта**: оба эти процесса завязаны на стандартизацию во всех ее формах. Когда капиталы и люди свободно мигрируют между странами, они, разумеется, ожидают применения в этих странах единых стандартов: мер, весов, размеров, напряжений в энергосетях, сопряжений зарядных устройств и т.д.

Когда люди общаются, торгуют, обмениваются разного рода услугами по глобальным сетям, то они ожидают, что регулирование этой их деятельности должно быть одинаковым во всех странах, охваченных процессами цифровизации.

Однако в этой сфере движения в одну сторону – в сторону позитива – пока не наблюдается. В чем-то страны сближаются, в чем-то, наоборот, расходятся. К примеру, весь мир сейчас торгует нефтью в бочках (баррелях) и за доллары. Однако напряжение в электросетях в Европе 220 вольт, а в Америке – 110 вольт. В России одна ширина колеи железных дорог, а в Западной Европе – другая. В Европе правостороннее движение по автодорогам, а в Великобритании – левостороннее. В Европе литры и метры, а в Англии и США – галлоны и футы. И так далее.

Разумеется, все эти расхождения мешают жизни людей в сопредельных странах, тормозят движение глобальных процессов во всех сферах бизнеса и финансов.

И еще неприятнее то, что в некоторых очень важных сферах международного общения имеет место противоположный вектор движения. Чуть больше века назад люди ездили из страны в страну без всяких виз, а сейчас на каждое пересечение государственной границы надо особое разрешение. При этом некоторые группы стран общение своих народов облегчают – отменяют границы для миграций между этими странами, но для людей из других стран создают особые визовые преграды. Интересно, что демократические по сути – например, страны Евросоюза – льготы людям из других стран предоставляют на самых антидемократических основах. Есть особые льготы в этих странах для дипломатов, депутатов, госслужащих, для обладателей «золотых вкладов», но на простых людей эти льготы не распространяются.

Также век назад люди из стран с валютами, основанными на золотом стандарте, перемещались по всему миру, не заботясь ни о каких валютных обменах (тогда говорили, что для британца пропуск для путешествий по всему миру есть английский фунт стерлингов), сегодня все заботятся об изменениях курсов валют. В Евросоюзе эту проблему решили, а американцы просто перестали ездить за границу: по официальным данным на сегодняшний день 50 % американцев не

имеют паспорта (заграничного, поскольку внутренних паспортов в США нет), а 30 % вообще никогда не выезжали за пределы США.

В цифровизации приходится интенсивно заимствовать некоторые иностранные технологии, а это отражается на ее безопасности и суверенитете.

## ВОПРОСЫ ДЛЯ САМОКОНТРОЛЯ

1. Технологии защиты электронного бизнеса от внешних угроз.
2. Развитие цифровой экономики как фактор изменения принципов конкурентных отношений хозяйствующих субъектов.
3. Противоречия рынка труда и технологий цифровой экономики: угроза безработицы и дефицит кадров.
4. Основы информационной безопасности в условиях цифровизации экономики.
5. Проблема защиты персональных данных: угроза мошенничества при расширении цифрового сервиса и индивидуализации видов услуг.
6. Основы обеспечения безопасности информационных систем государственных структур.
7. Риски цифровой идентификации.