ФГБОУ ВО «ЧЕЧЕНСКИЙ ГОСУДАРСТВЕННЫЙ
ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Л.Х. Джабраилова**

# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК ПРИОРИТЕТНОЕ НАПРАВЛЕНИЕ РАЗВИТИЯ ЦИФРОВОЙ ЭКОНОМИКИ

***Монография***

**Махачкала - 2020**

УДК 330.322, 338.2, 658
ББК 32.97, 65.05
Д-40

*Печатается по решению Ученого Совета Чеченского государственного педагогического университета*

***Рецензенты:***

**Исраилов М.В.** д.э.н., профессор кафедры «Менеджмент и государственное и муниципальное управление» Чеченского государственного университета;

**Эльдерханов Х-М.Ю.** д.э.н., профессор, действительный член (академии) Российской академии естествознания, профессор кафедры «Экономика и управление в образовании» Чеченского государственного педагогического университета.

**Джабраилова Л.Х.**

**Д-40** Информационная безопасность как приоритетное направление развития цифровой экономики. – Махачкала: АЛЕФ, 2020. – 118 с.

ISBN 978-5-00128-612-7

В современных условиях социально-экономического развития России важнейшим аспектом обеспечения устойчивого развития экономики и обеспечения ее безопасности является цифровизация экономики. В монографии представлены результаты исследований, отражающие тенденции и перспективы развития и внедрения цифровых технологий в экономике. Анализируется роль процессов цифровой трансформации экономики в России. Особое внимание уделено исследованию факторов, влияющих формированию цифровой экономики в условиях глобализации и цифровой трансформации экономики. Также автором место отводится анализу угроз и рисков, которые сдерживают цифровизацию экономики.

Материалы монографии будут полезны преподавателям, научным работникам, специалистам разных отраслей промышленности, а также аспирантам и студентам.

**ОГЛАВЛЕНИЕ**

СПИСОК СОКРАЩЕНИЙ И УСЛОВНЫХ ОБОЗНАЧЕНИЙ ..... 4
ВВЕДЕНИЕ ..... 5
ГЛАВА 1. ПОНЯТИЕ, ОСНОВНЫЕ ЧЕРТЫ И МЕСТО ЦИФРОВОЙ ЭКОНОМИКИ В ЭВОЛЮЦИИ ХОЗЯЙСТВЕННОЙ ДЕЯТЕЛЬНОСТИ ..... 6
1.1. Основные предпосылки развития цифровой экономики ..... 6
1.2. Понятие, цели, задачи цифровой экономики ..... 10
1.3. Закономерности развития цифровой экономики ..... 28
1.4. Тенденции развития «цифровой экономики» в России ..... 40
1.5. Подготовка кадров для цифровой экономики и проблемы труда в условиях цифровизации ..... 49
ГЛАВА 2. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЦИФРОВОГО ПРОСТРАНСТВА КАК ПРИОРИТЕТНОЕ НАПРАВЛЕНИЕ РАЗВИТИЯ ЦИФРОВОЙ ЭКОНОМИКИ ..... 56
2.1. Информационная безопасность в системе национальной безопасности ..... 56
2.2. Информационная безопасность цифрового пространства Интернета вещей ..... 75
2.3. Основные меры противодействия угрозам информационной безопасности ..... 82
2.4. Риски и угрозы информационной безопасности ..... 85
ЗАКЛЮЧЕНИЕ ..... 104
ИСПОЛЬЗОВАННАЯ ЛИТЕРАТУРА ..... 105

# СПИСОК СОКРАЩЕНИЙ И УСЛОВНЫХ ОБОЗНАЧЕНИЙ

ИТ – информационные технологии
ИКТ – информационно-коммуникационные технологии
ИЭ – информационная экономика
ИО – информационное общество
ПО – программное обеспечение
ПК – персональный компьютер
ИИ – искусственный интеллект
ВР – виртуальная реальность
ЧК – человеческий капитал
АС – автоматизированные системы
ЭВМ – электронно-вычислительные машины
ИС – информационные системы
ИР – информационная революция
НТР – научно-техническая революция
НТП – научно-технический прогресс
ИБ – информационная безопасность
СМИ – средства массовой информации
АИС – автоматизированные информационные системы
БПЛА – беспилотные летательные аппараты
БМД – Большие массивы данных
ВВП – валовой внутренний продукт
ЮНЕСКО – специализированное учреждение ООН по вопросам образования, науки и культуры
ОЭСР – Организация экономического сотрудничества и развития
ЕАЭС – Евразийский экономический союз
РАЭК – Российская ассоциация электронных коммуникаций
НИОКР

# ВВЕДЕНИЕ

В настоящее время в век компьютеризации и высоких технологий цифровая экономика затрагивает каждый аспект жизни: здравоохранение, образование, интернет-банкинг, правительство. Цифровая экономика получила развитие во всех высокоразвитых странах, в том числе и в России.

Исходя из событий внешней политики и общемировых тенденций перед Россией стоит вопрос глобальной конкурентоспособности и национальной безопасности, и не малую роль в решении данного вопроса играет развитие цифровой экономики в стране. Некоторые элементы цифровой экономики уже успешно функционируют. На сегодня, учитывая массовый перенос документов и коммуникаций на цифровые носители, разрешение электронной подписи, общение с государством также переходит на электронную платформу.

Автор данной монографии анализирует причины цифровизации, рассматривает причины и цели появления цифровой экономики, анализирует методы и технологии, способствующие поддержке функционирования цифровой экономики.

Целью работы является: определение и идентификация основных технологических трендов в сфере цифровой трансформации экономики России, факторов влияния на эффективность цифровой экономики, изучение вопросов обеспечения экономической и информационной безопасности России как приоритетного направления цифровой экономики.

Методическую основу исследования составили положения о системном, обобщённом, аналитическом и сравнительном подходах. В рамках анализа использованы методы и инструменты моделирования, а также методы экономико-статистического анализа.

В исследовании выявлены и раскрыты основные факторы информационной безопасности страны в контексте развития цифровизации экономики.

Полученные результаты целесообразно применять при разработке документов стратегического планирования и реализации государственных программ экономического развития в целях обеспечения национальной и информационной безопасности России.

Материалы монографии будут полезны преподавателям, научным работникам, специалистам разных отраслей промышленности, а также аспирантам и студентам.

# ГЛАВА 1. ПОНЯТИЕ, ОСНОВНЫЕ ЧЕРТЫ И ТЕНДЕНЦИИ РАЗВИТИЯ ЦИФРОВОЙ ЭКОНОМИКИ

## 1.1. Основные предпосылки развития цифровой экономики

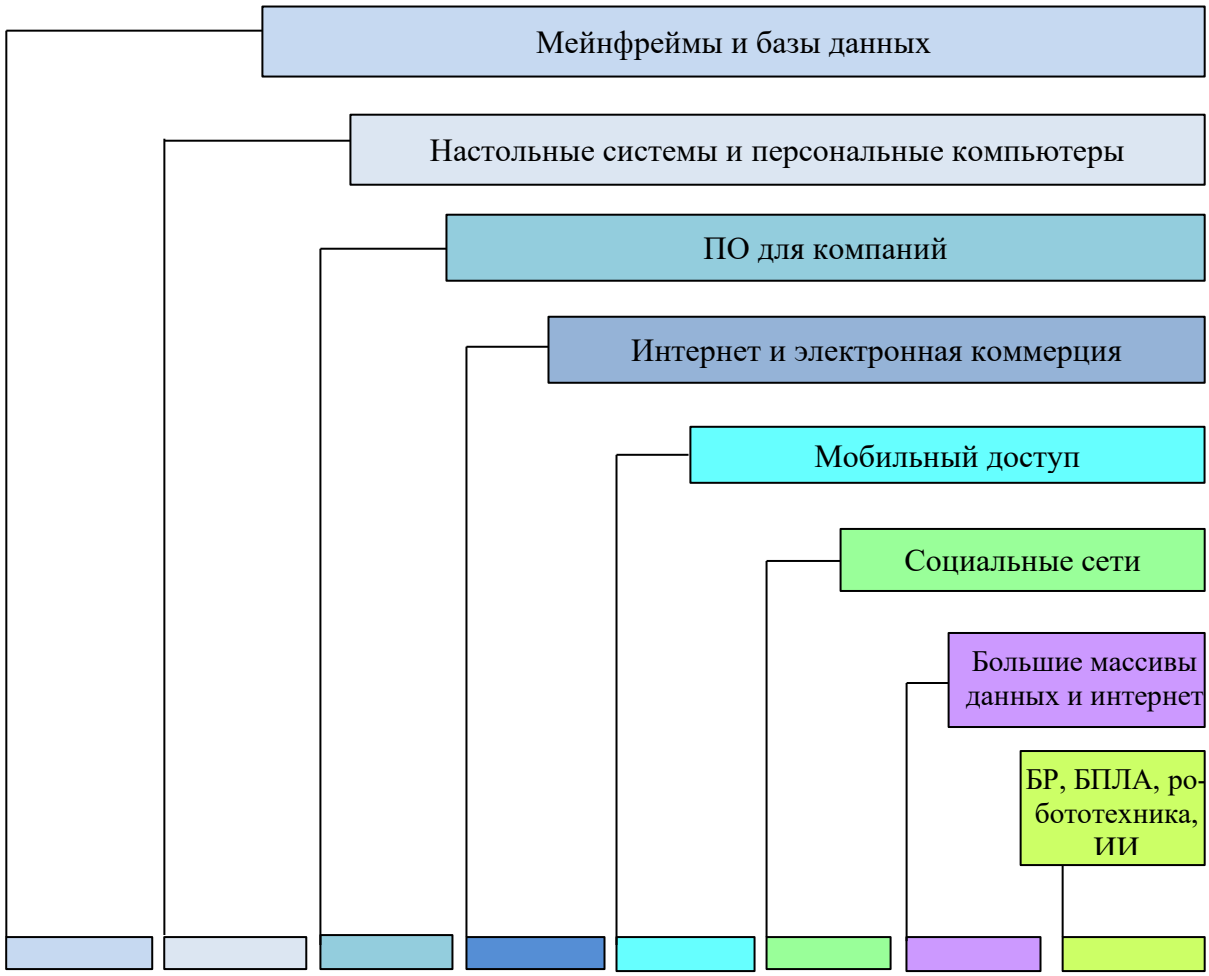
Впервые понятие «цифровая экономика» упоминается более 20 лет назад американским информатиком Николасом Негропонте. Преимуществами цифровой экономики как «нового» вида экономики, на взгляд информатика, могли стать: отсутствие физического веса продукции, заменяемого информационным объемом, более низкие затраты ресурсов на производство электронных товаров, в несколько раз меньшая площадь, занимаемая продукцией (как правило электронными носителями), а также мгновенное глобальное перемещение через сеть Интернет [126].

В России это понятие раскрыто в Стратегии развития информационного общества, утвержденной в мае 2017 года [1]. Стратегия развития информационного общества выделяет цифровую экономику как один из шести национальных интересов [1].

Несомненно, что в современном мире словосочетание «цифровая экономика», стало упоминаться все чаще и чаще. Похоже, что новые технологии, которые активно развиваются в мировом масштабе, скоро перевернут наше представление о возможностях. Взрывной рост социальных сетей, рынка смартфонов, широкополосного доступа к интернету, технологий машинного обучения и искусственного интеллекта меняют мир. В связи с этим, правомерно будет рассмотреть истоки зарождения, становления и развития цифровой экономики [6].

Цифровая революция, охватившая мировую экономику, впечатляет масштабом, темпами и географией. Начиная с 1960-х годов цифровые инновации распространялись по миру сменявшими друг друга волнами, исходившими из научных эпицентров США, Европы и СССР (Рисунок 1).

Каждый из этих этапов был интенсивнее предыдущих, охватывая новые регионы и оказывая все более ощутимый для экономики эффект. Переход от больших ЭВМ к ПК длился десятилетия, сейчас революционные перемены происходят за годы и месяцы. Первый этап цифровых инноваций сводился к автоматизации существующих технологий и бизнес-процессов. Второй этап начал формироваться в середине 1990-х годов, когда распространение интернета, мобильной связи, социальных сетей, появление смартфонов привели к стремительному росту использования технологий конечными потребителями.




Современные языки программирования.

Базовое офисное ПО ПК. Обработка документов. Хранилище файлов. Игры.

Корпоративное ПО. Автоматизация бизнес-процессов.

Интернет-технологии. Интернет-торговля. Электронная почта и часы.

GPS, Wi-Fi, ноутбуки, мобильные телефоны.

Социальные сети, смартфоны, цифровая реклама и маркетинг.

Большие массивы данных и интернет. Прогнозная аналитика. Интернет вещей. Индустрия 4.0

Прогнозные алгоритмы. Машинное обучение. ВР. БПЛА. Робототехника.

ВР - Виртуальная реальность

БПЛА - Беспилотные летательные аппараты

ИИ – искусственный интеллект

**Рисунок 1** – Цифровая революция

Цифровые технологии меняют саму операционную модель компаний, особенно в банковских и телекоммуникационных секторах, повышают эффективность затрат и выявляют новые возможности на рынке. В традиционных отраслях активно применяются методы анализа больших объемов данных для получения новых знаний и принятия эффективных управленческих решений. В современном мире такое явление получило название «цифровая экономика» [43].

Большое количество новых терминов, которое употребляется авторами многочисленных публикаций о цифровых технологиях, приводят к сложностям в понимании сущности явления цифровой экономики. Для определения как понятия «цифровая экономика», правомерным будет обратиться к формулировке семинара Всемирного банка 20 декабря 2016 г. [92], где цифровая экономика была определена как парадигма ускорения экономического развития с помощью цифровых технологий. Это определение, как и многие другие известные определения, прежде всего, имеют в виду использование ИКТ.

Цифровую экономику правомерно рассматривать как составную часть шестого технологического уклада и четвертой промышленной революции, что объясняется следующими соображениями. Все наши действия в ВР можно отнести к системе производства, распределения, обмена или потребления. Но ВР появилась не с созданием компьютера. Вся мыслительная деятельность человека может быть отнесена к ней [7].

Другой профессор РАН, доктор технических наук Роман Мещеряков считает, что к термину «цифровая экономика» существует два подхода. Первый подход «классический»: цифровая экономика – это экономика, основанная на цифровых технологиях и при этом правильнее характеризовать исключительно область электронных товаров и услуг. Примеры – телемедицина, дистанционное обучение, продажа медиконтента (кино, ТВ, книги и пр.). Второй подход – расширенный: «цифровая экономика» – это экономическое производство и использованием цифровых технологий» [122].

Концепция цифровой экономики появилась в последнем десятилетии 20 века. Одним из ученых, сформулировавших основополагающие принципы цифровой экономики, был Николас Негропонте – специалист в области информатики, основатель медиа лаборатории Media Labs Массачусетского технологического института (MIT). В 1995 году он говорил о недостатках классических товаров (вес, сырье, транспорт) и преимуществах новой экономики (отсутствие веса товаров, виртуальность, почти не нужное сырьё, мгновенное глобальное перемещение)

[136]. В 1999 году Билл Гейтс в своей книге «Бизнес со скоростью мысли» конкретизировал идеи информационной революции. Согласно его мнению, развитие ИТ оказывает значительное влияние на все стороны жизни общества. При этом современный бизнес обязан быстро реагировать на изменения и вызовы «новой экономики», такие, как растущие потребности клиентов и обострение конкуренции. Он пишет: «В будущем на рынке останется два вида компаний: те, кто в Интернете, и те, кто вышел из бизнеса» [25].

Способов по развитию «цифровой экономики» оказалось много, так как каждый из них преследует концепцию глубокой интеграции ИТ с реальными процессами экономики. Цифровая экономика формируется с ориентацией на потребителя, места реализации и цены, которая должна соответствовать качеству предоставляемой услуги [26]. Сегодня мир находится на пути перехода на этап постиндустриальной цифровой экономики, который способен кардинально изменить мировой рынок:

- главным ресурсом станет информация [48].
- торговые площадки в интернете не ограничены [51].
- организации способны конкурировать с более крупными игроками рынка [37].
- масштаб операционной деятельности ограничен только размером Интернета [70].

На протяжении первых 10 лет базой цифровой экономики являлись бизнес электронной торговли и сервиса. В дальнейшем уровень представляемых сервисов значительно изменился, объединив ранее разрозненные технологии. На фоне этого произошло формирование абсолютно новых подходов в управлении производственными процессами.

Примером построения системы цифровой экономики, которая связана с технологиями информационного моделирования, стала «информационная модель здания» – BIM. Данная модель явилась революционной, позволив одновременно объединить подходы к проектированию, возведению, оснащению, эксплуатации и ремонту объектов строительной отрасли Британии в единой базе данных. Дополнительным результатом данной модели в дальнейшем стала консолидация исследований и разработок «киберфизических систем» – CPS. Под киберфизическими системами принято понимать умные системы, включающие интерактивные инженерные сети, такие как «интернет вещей». Вся суть киберфизических систем заключается в том, что объединяют

физический процесс производства, которые требуют бесперебойной работы в режиме «online», с программно-электронными системами [33].

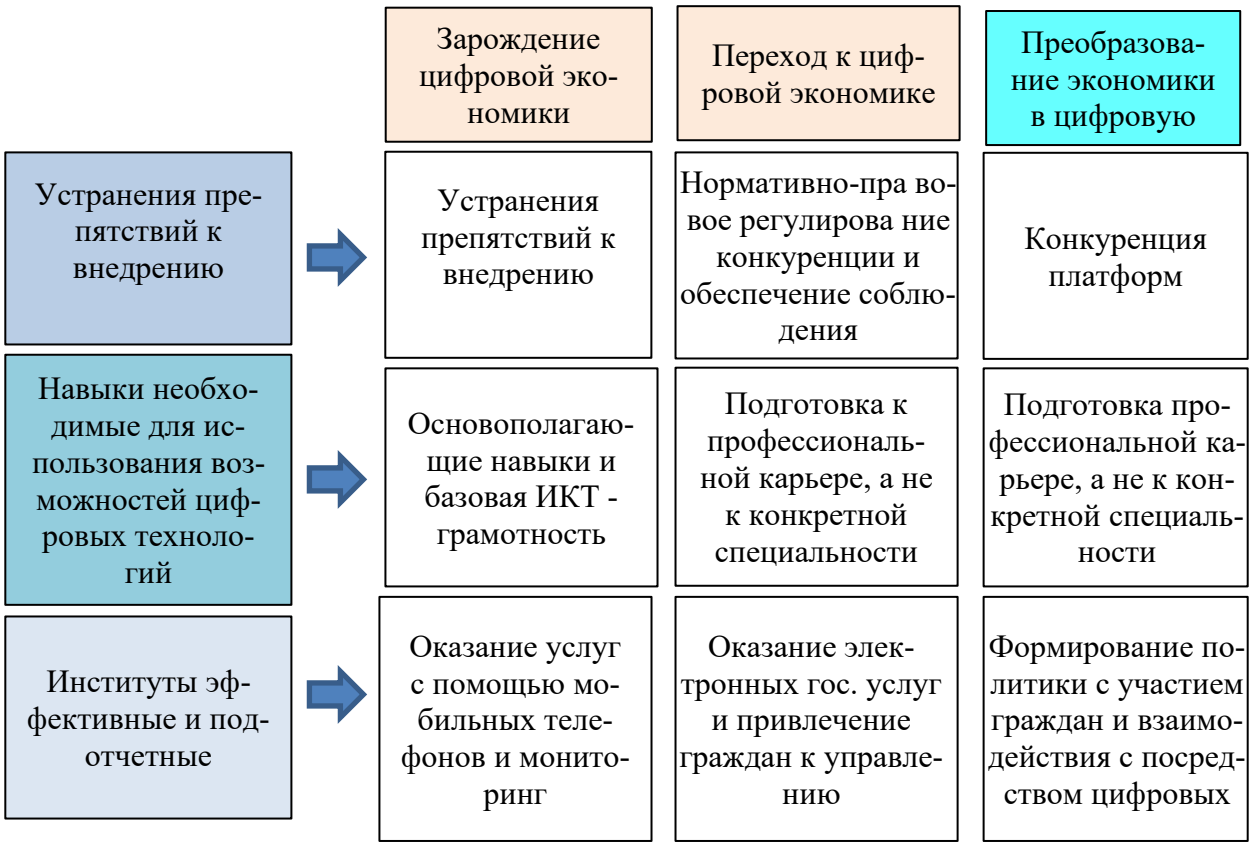



**Рисунок 2** – Стратегические приоритеты цифровой экономики

## 1.2. Понятие, цели, задачи цифровой экономики

Цифровые технологии становятся повседневной частью экономической, политической и культурной жизни, хозяйствующих субъектов Российской Федерации и двигателем развития общества в целом. Россия стоит на прогрессивном этапе развития современной цивилизации, который характеризуется доминированием знаний, науки, технологий и информации во всех жизнедеятельности. Исходя из событий внешней политики и общемировых тенденций, перед Россией стоит вопрос глобальной конкурентоспособности и национальной безопасности, и не малую роль в решении данного вопроса играет развитие цифровой экономики в стране. Некоторые элементы цифровой экономики уже успешно функционируют. На сегодня, учитывая массовый перенос документов и коммуникаций на цифровые носители, разрешение

электронной подписи, общение с государством также переходит на электронную платформу [52].

Термин «информационная экономика» впервые был озвучен еще в 1976 г. сотрудником Стэнфордского центра междисциплинарных исследований М. Поратом и стал массовым после выхода в 1996-1998 гг. знаменитой книги М. Кастельса «Информационная эпоха: экономика, общество и культура» (русский перевод сделан в 2000 г.), в которой он писал, что производительность и конкурентоспособность факторов или агентов (будь то индивид, фирма или национальная экономика) зависят, в первую очередь, от их способности генерировать, обрабатывать и эффективно использовать информацию, основанную на знаниях [44, с. 81].

Главная движущая сила информационной экономики – не производство и потребление материальных благ, а производство и потребление информации как в овеществленной форме (продукты высоких технологий), так и в невещественной, становясь в результате не только основополагающим фактором развития экономики, но и всего общества в целом [77].

Информационная экономика, основанная на информации, постепенно трансформируется в экономику, основанную на знаниях, в которой основным продуктом экономики становится уже не сама информация, а знания и обладание ими. В связи с этим наиболее ценными становятся не те сотрудники, которые имеют доступ к информации, а сотрудники, обладающие определенным набором знаний [130]. Так возникло новое понятие «экономика, основанная на знаниях», или «экономика знаний» (Knowledge Economy), которая создает, распространяет и использует знания для обеспечения своего роста и конкурентоспособности. Это такая экономика, в которой знания обогащают все отрасли, все сектора и всех участников экономических процессов. Это экономика, которая использует знания для создания высокотехнологичной продукции, высококвалифицированных услуг, научной продукции и образования.

Экономика знаний постепенно трансформируется в креативную экономику – особый сектор экономики, основанный на интеллектуальной деятельности, основными характеристиками его являются: высокая роль новых технологий и открытий в разных областях деятельности человека; высокая степень неопределённости; большой объем уже существующих знаний и острая необходимость генерации новых знаний [76, с. 585]. Креативная экономика основана на интеллектуальной деятельности, характеризуется наращиванием в обществе креативных

ценностей путем развития творчества и благоприятствующих ему условий. В совместном Докладе ЮНЕСКО отмечено, что структура креативной экономики существенно отличается от структуры экономики индустриального общества; в ее сферу входят развитие аудиовизуальных процессов, реклама, дизайн, архитектура, декоративное искусство, мода, новые средства массовой информации, сценическое искусство, издательское дело, репродуцирование произведений искусства и т. д. Эти отрасли трактуются как быстро растущие сектора и как важные источники доходов, которые вносят огромный вклад в расширение рынка занятости и способствуют росту экспортных поступлений [59]. Результатом развития этих отраслей является закрепление и преумножение на национальном уровне авторских прав, патентов, торговых марок и т. д.

Креативную экономику отличают непрерывное инновационное развитие, опора на человеческий капитал, инвестиции в новые технологии и проектные разработки, высокая наукоемкость производства продукции, преобладающая доля наукоемкой продукции в ВВП стран, высокая конкурентоспособность, специализация и координация субъектов хозяйственной деятельности, комплексное производство, имеющее межотраслевой характер, высокий уровень образования и профессиональной подготовки работников индустрий, наконец, правовая защита интеллектуального капитала. Креативные индустрии можно трактовать как особый тип социально-культурных практик, где основной интегрирующей доминантой выступает креативная компонента [135].

В условиях массового использования информационных сетей, прежде всего, интернета, возникли понятия «интернет-экономика» и «сетевая экономика». Под интернет-экономикой (Internet Economy) Е. В. Красильникова понимает «…любую хозяйственную деятельность, в основе которой лежат специфические экономические отношения между людьми в сфере создания, распределения, обмена и потребления информационных ресурсов (продуктов) с использованием глобальной сети Интернет» [58, с. 33].

С. Дятлов под сетевой экономикой понимает глобальную сетевую многоуровневую структуру взаимоотношений между экономическими агентами посредством интернета и других телекоммуникационных средств, развивающуюся в соответствии со своими специфическими целями и критериями эффективности [35]. Он предлагает зафиксировать термин «netnomics» за теорией сетевой экономики, включающей в себя собственный предмет и метод исследования, а также

методы управления электронно-сетевыми взаимодействиями, инструментарий принятия решений и проведения практической политики в сфере электронно-сетевой экономики.

Развитие сектора ИКТ, увеличение темпов электронизации общественных и государственных систем, расширение промежуточного потребления ИКТ-продуктов всеми отраслями экономики указывают на необходимость введения термина «электронная экономика» как совокупности экономических отношений в области производства, распределения, обмена и конечного потребления материальных ценностей, имеющих разную степень электронно-информационного компонента, формируемых и реализуемых в ИКТ-среде с целью воспроизводства капитала и повышения качества жизни [85].

Электронная экономика как новый тип экономической системы характеризуется:

- увеличением автономности (от человека как субъекта управления) механизма управления, а именно стремлением к расширению роботизации процесса управления (в том числе принятия решения) экономикой;
- типом потребляемого дополнительного ресурса (данные, интеллектуальный ресурс, ресурс телекоммуникационных сетей и ИТ);
- постоянным изменением правил и технологий функционирования системы;
- увеличением экономической зависимости от электронных компонентов, в том числе от данных, накапливаемых и передаваемых с их помощью, и от ИТ, принадлежащих третьим лицам;
- главенствующей ролью науки и ИКТ в производстве;
- открытостью данных, коммерческой информации, технологий;
- проектированием хозяйственной деятельности как мультикультурной и межгосударственной системы;
- расширением функций инновационного менеджмента (наращиванием скоростей управляемых изменений).

Термин «новая экономика» («неоэкономика») появился в начале 1980-х гг. и использовался тогда для описания экономики, которая в большей степени опирается на сферу производства услуг, чем на сферу производства товаров.

В новой экономике происходит широкое внедрение ИКТ. По определению Совета доступа США, ИКТ – это любая информационная технология, оборудование, интегрированные системы или подсистемы оборудования, функциональным назначением которых является создание, преобразование, копирование, автоматический сбор и обработка,

хранение и анализ, манипулирование, управление, перемещение и контроль, воспроизведение, коммутация, обмен, передача, прием, и трансляция данных или информации (электронный контент, телекоммуникационные продукты, компьютеры и вспомогательное оборудование, программное обеспечение, информационные киоски и транзакционные автоматические устройства, видео, ИТ-сервисы, многофункциональное офисное оборудование, предназначенное для копирования, сканирования и факсимильной передачи документов [151, p. 8].

Академик В. Л. Макаров сформулировал термин «новая экономика» следующим образом: «это тип экономики, где сектора технологической материализации знаний играют решающую роль, а производство знаний является источником экономического роста» [69, с. 4].

Внедрение ИКТ увеличивает ценность связей между экономическими субъектами, резко повышает гибкость и снижает стоимость транзакций, в результате чего изменяется соотношение значимости факторов производства: если в прошлом основными факторами производства были труд, земля и капитал, то в новой экономике основополагающим ресурсом становятся знания в широком смысле (данные, информация, символы, культура, идеология и ценности) [113].

Новая экономика охватывает всю систему макроэкономических последствий развития новых технологий, например, влияет на динамику фондового рынка с сопутствующими изменениями в структуре богатства и доходов юридических и физических лиц; воздействует на темп экономического роста и на производительность труда в отраслях.

***Таблица 1***

**Соотношение параметров различных феноменов современной глобальной экономики**

| Тип экономики | Основной фактор производства | Основные блага | Основной экономический ресурс | Источник богатства | Тип экономических отношений |
|---|---|---|---|---|---|
| Информационная экономика | Информация | Информация | Информационный капитал | Информационная рента | Вертикальные |
| Экономика знаний | Знания, инновации | Знания | Интеллектуальный, | Информационная, | Вертикальные |

| | | | | | |
|---|---|---|---|---|---|
| | | | «структурный» капитал | интеллектуальная рента | |
| Креативная экономика | Креативный потенциал | Интеллектуальные права | Креативный капитал | Интеллектуальная рента | Вертикальные |
| Интернет-экономика | Информация | Информация | Информационный капитал | Информационная рента | Вертикальные |
| Сетевая экономика | Информация | Сетевые блага | Информационный капитал | Информационная рента | Вертикальные |
| Электронная экономика | Информация | Информация | Информационный капитал | Информационная рента | Вертикальные |
| Новая экономика | Информация, знания, технологии, инновации | знания, технологии, инновации | Информационный, интеллектуальный капитал | Технологическая, интеллектуальная рента | Горизонтальные |
| Цифровая экономика | Информация, знания, ИКТ, инновации | Информация, знания, технологии, инновации | Информационный, интеллектуальный, «структурный» капитал | Технологическая, интеллектуальная, информационная рента | Горизонтальные |

Источник: [27].

Следовательно, это понятие не исчерпывается информационным аспектом, а представляет качественно новый технологический уровень всего народного хозяйства, включая действующие производительные силы общества [105].

Цифровая экономика появилась как обобщающее понятие, содержащее не только признаки всех перечисленных экономик, но и ряд более общих отличительных черт, характеризующих качественную определенность цифровой экономики (Таблица 1).

Несмотря на значительное число работ, посвященных обсуждению феномена цифровой экономики, до сих пор нет однозначного

понимания того, что представляет собой цифровая экономика как социально-экономическая система.

Как признают участники исследования за 2017 г., проведенного международной консалтинговой компанией PricewaterhouseCoopers, само определение понятия «цифровой экономики» постоянно меняется.

Сравнительный анализ различных определений цифровой экономики международными организациями представлен в таблице 2.

***Таблица 2***

**Список определений понятия «цифровая экономика» международными организациями**

| Автор | Определение |
|---|---|
| ОЭСР (2012) | Цифровая экономика делает возможным и задействует торговлю товарами и услугами посредством электронной торговли в сети Интернет [137]. |
| Департамент коммуникаций и цифровой экономики Австралии (2013) | Цифровая экономика – глобальная сеть экономических и социальных мероприятий, реализуемых через такие платформы, как интернет, а также мобильные и сенсорные сети [138]. |
| Британское компьютерное сообщество (2014) | Цифровая экономика – это экономика, основанная на цифровых технологиях, однако мы в большей степени под этим понимаем осуществление операций на рынках через интернет-сети [139]. |
| ОЭСР (2015) | Цифровая экономика есть результат трансформационных эффектов новых технологий в области информации и коммуникации [140]. |
| Европейский Парламент (2015) | Цифровая экономика – сложная структура, состоящая из нескольких уровней/слоев, связанных между собой практически бесконечным и постоянно растущим количеством узлов. Платформы существуют во взаимосвязи, позволяя достичь непосредственного пользователя через множества каналов, тем самым усложняя исключение конкретных игроков, то есть конкурентов [141]. |
| Всемирный банк (2016) | Цифровая экономика – новая парадигма ускоренного экономического развития, основанная на обмене данными в режиме реального времени. Это система экономических, социальных и культурных отношений, основанных на использовании цифровых ИКТ [92]. |

| | |
|---|---|
| ОЭСР (2016) | Цифровая экономика – сочетание технологий общего применения и некоторых видов экономической и общественной деятельности, осуществляемых пользователями интернета при помощи соответствующих технологий. Цифровая экономика включает в себя физическую инфраструктуру, которую задействуют цифровые технологии (широкополосные сети, маршрутизаторы), устройства доступа (компьютеры, смартфоны), информационные системы (Google, Salesforce) и обеспечиваемый ими функционал (анализ больших данных, интернет вещей, облачные вычисления) [142]. |
| TechTarget (2016) | Цифровая экономика есть всемирная сеть видов экономической деятельности, которые стали доступными благодаря ИКТ. Это экономика, основанная на цифровых технологиях [143]. |
| G20 (2016) | К цифровой экономике относятся самые различные виды экономической деятельности, в которых использование цифровой информации и знаний играет роль ключевого фактора производства, современные информационные сети становятся важной сферой деятельности, а эффективное применение ИКТ выступает как важная движущая сила оптимизации и повышения результативности экономики [39]. |
| Конференция ООН по торговле и развитию (2017) | Цифровая экономика – это применение цифровых интернет-технологий в процессе производства товаров и услуг и торговли ими [144]. |
| Deloitte (2017) | Цифровая экономика – это форма экономической активности, которая возникает благодаря сетевому взаимодействию людей, предприятий, устройств, данных и процессов. Основой цифровой экономики является связуемость, то есть растущая взаимосвязанность людей, организаций и машин, формирующаяся благодаря интернету, мобильным технологиям и интернету вещей [145]. |
| Oxford Dictionary (2017) | Цифровая экономика – экономика, которая функционирует в основном за счет применения цифровых технологий, в частности безналичных операций через интернет [146]. |

| | |
|---|---|
| Институт глобального развития (Университет Манчестера) (2018) | Цифровая экономика – часть общего объема производства, которая целиком или в основном произведена на базе цифровых технологий фирмами, бизнес-модель которых основывается на цифровых продуктах или услугах [20]. |

Наряду с появлением новых тенденций и закономерностей, ранее не имевших место в индустриальной и постиндустриальной экономике, следует обратить внимание на новое содержание установившихся экономических положений, которые в сочетании и взаимосвязи с цифровыми технологиями проявляют себя по-новому. Цифровая экономика – это не только новые цифровые технологии, но также значительные изменения в традиционных правилах ведения бизнеса, в новых проявлениях классических экономических закономерностей [22]. Появление и распространение глобальных коммуникационных сетей, персональных компьютеров, электронных продуктов и услуг, объединяемых термином «цифровые технологии», решительным образом изменяет в цифровой экономике содержание, значение и соотношение следующих понятий: материального и нематериального, местоположения и расстояния, времени и пространства, потребительной стоимости и полезности, качества и количества, потребительского спроса и конкуренции, посредничества и логистики, человеческого капитала и этики бизнеса, сделок и оценки эффективности, поведения продавцов и покупателей, новых взаимоотношений производителей и потребителей, технологий маркетинга и сбыта и т. д. [31].

В основных публикациях российских исследователей по рассматриваемой теме периода 2014-2018 гг. определения термина «цифровая экономика» существенно отличаются друг от друга, причём понятие цифровой экономики в большинстве случаев рассматривается в более узком смысле, чем в публикациях и исследованиях зарубежных авторов (Таблица 3).

***Таблица 3***

**Список определений понятия «цифровая экономика» российскими авторами**

| Автор | Определение |
|---|---|
| Указ Президента РФ от 09.05.17 г. №203 «О | Цифровая экономика – хозяйственная деятельность, в которой ключевым фактором производства являются данные в цифровом виде, обработка |

| | |
|---|---|
| Стратегии развития информационного общества в РФ на 2017-2030 годы» | больших объемов и использование результатов анализа которых по сравнению с традиционными формами хозяйствования позволяют существенно повысить эффективность различных видов производства, технологий, оборудования, хранения, продажи, доставки товаров и услуг [1]. |
| Программа развития цифровой экономики в России до 2035 г. | Цифровая (электронная) экономика – совокупность общественных отношений, складывающихся при использовании электронных технологий, электронной инфраструктуры и услуг, технологий анализа больших объёмов данных и прогнозирования в целях оптимизации производства, распределения, обмена, потребления и повышения уровня социально-экономического развития государств [93]. |
| В.М. Бондаренко | Цифровая экономика есть целостная, системная, комплексная проблема нахождения той модели отношений между людьми, которая совместима с технологиями четвертой промышленной революции, то есть с цифровыми технологиями и другими высокими технологиями XXI века и в своем формировании, развитии и реализации должна обеспечивать достижение объективно заданной цели [17, с. 238]. |
| В. Иванов | Цифровая экономика – это виртуальная среда, дополняющая нашу реальность [109]. |
| Р. В. Мещеряков | К термину «цифровая экономика» существует два подхода. 1. (классический): цифровая экономика – экономика, основанная на цифровых технологиях, и при этом правильнее характеризовать исключительно область электронных товаров и услуг (телемедицина, дистанционное обучение, кино, ТВ, книги и пр.).<br>2. (расширенный): цифровая экономика – экономическое производство с использованием цифровых технологий [109]. |
| А. А. Энговатова | Цифровая экономика – экономика, основанная на новых методах обработки, хранения, передачи данных, а также цифровых компьютерных технологиях. В рамках данной модели кардинальную трансформацию претерпевают существующие рыночные бизнес-модели, существенно меняется формирование добавочной стоимости, значение посредников всех уровней в экономике резко |

| | |
|---|---|
| | сокращается. Увеличивается значение индивидуального подхода к формированию продукта, – ведь теперь мы можем смоделировать все, что угодно [109]. |
| М. Л. Калужский, директор Фонда региональной стратегии развития | Цифровая экономика – это коммуникационная среда экономической деятельности в сети интернет, а также формы, методы, инструменты и результаты ее реализации [42, с. 75]. |
| А. А. Кунцман | Цифровая экономика представляет собой современный тип экономики, характеризующийся преобладающей ролью информации и знаний как определяющих ресурсов в сфере производства продуктов и услуг, а также активным использованием цифровых технологий хранения, обработки и передачи информации [62, с. 2]. |
| Р. К. Асанов | Цифровая экономика есть экономика, основанная на производстве электронных товаров и сервисов высокотехнологичными бизнес-структурами и дистрибуции этой продукции при помощи электронной коммерции [9, с. 144]. |
| И. П. Бойко, М. А. Евневич, А. В. Колышкин. | Цифровая экономика представляет собой совокупность видов деятельности, базирующихся на цифровых технологиях, а также инфраструктура, которая обеспечивающую функционирование этих технологий. Под цифровыми технологиями следует понимать технологии, связанные с созданием, сбором, обработкой, хранением и передачей информации на основе цифровых систем [16, с. 1131]. |
| Е. Б. Стародубцева, О. М. Маркова. | Под цифровой экономикой мы понимаем совокупность отраслей, связанных с появлением новых технологий, развитием робототехники, в которых применяются цифровые платформы, новые технологии, робототехника, смарт-технологии и т. д. [106, с. 7]. |
| С. А. Плуготаренко | Экосистема цифровой экономики – сегменты рынка, где добавленная стоимость создается с помощью цифровых ИТ [38, с. 297]. |
| В. К. Крутиков | Цифровая экономика – это системная совокупность экономических отношений по поводу производства, распределения, обмена и потребления товаров и услуг техноцифровой формы существования. Техноцифровая природа экономических |

| | |
|---|---|
| | отношений – ключевой отличительный признак цифровой экономики [60, с. 104]. |
| К. Варламов | Цифровая экономика – это уклад, в котором происходит системный и последовательный перевод в цифровой вид традиционных форм деловых и производственных отношений, форм взаимодействия на селения и предприятий с государством» [121, с. 2]. |
| Г. А. Гасанов, Т. А. Гасанов | Цифровая экономика – это система институциональных категорий (понятий) в экономике, базирующаяся на передовых научных достижениях и прогрессивных технологиях, прежде всего в ИКТ, функционирование которой направлено на увеличение эффективности производства, под держание устойчивых темпов роста экономики с целью повышения благосостояния и качества жизни граждан страны [24, с. 6]. |

Можно сделать вывод о том, что цифровая экономика – это не просто экономическая деятельность по производству цифровых (виртуальных) товаров и сервисов, а экономика, в которой повышение показателей ее функционирования достигается за счет расширения удовлетворения потребностей клиентов, интегрированных в цифровые процессы; развития инновационного сотрудничества на рынках с использованием информационных сетей для создания цифровых экосистем; технологического совершенствования продуктов и услуг на основе цифровых решений; цифровой реструктуризации бизнес-процессов и организационных форм управления компаниями.

Цифровая экономика, по мнению этих исследователей, – это экономика, существующая в условиях гибридного мира. Авторы сознательно используют кавычки при написании термина «цифровая» экономика, так как в их видении нет такого явления как «цифровая» экономика, которое было бы отделено от остальной экономики.

Самая широкая трактовка определения цифровой экономики, подразумевающая под ней виртуальную среду, дополняющую нашу реальность, содержит больше вопросов о данном феномене, чем ответов: можно ли все действия в компьютерной виртуальной реальности отнести к системе производства, распределения, обмена или потребления; можно ли утверждать, что в виртуальной среде воспроизводится традиционный экономический цикл, все его фазы в той же

последовательности и в тех же проявлениях, что и в реальной экономике? Эти вопросы требуют отдельного серьезного исследования [47].

Вместе с тем представляется, что нельзя сужать предмет цифровой экономики до сферы производства, распределения и потребления научно-технической информации посредством цифровых технологий. Кроме того, цифровую экономику невозможно ограничивать лишь чисто цифровыми продуктами и услугами, не имеющими материальной формы, вроде онлайн-продаж фильмов, музыки и книг или программного обеспечения.

Таким образом, как видно из большинства приведенных определений цифровой экономики, их неотъемлемой частью является признание ведущей роли ИКТ (прежде всего, интернета) в современной экономике. Фактически все сферы человеческой жизнедеятельности (экономическая, социальная, политическая, культурная, социальная и другие) в той или иной мере изменились благодаря открытию сетей и развитию ИКТ, однако именно изменения последних лет позволяют многим утверждать, что начинается новый этап информатизации, название которому «цифровая экономика».

Цифровая экономика – это система социальных, экономических и технологических отношений между государством, бизнес-сообществом и гражданами, функционирующая в глобальном информационном пространстве, посредством широкого использования сетевых ИТ генерирующая цифровые виды и формы производства и продвижения к потребителю продукции и услуг, которые приводят к непрерывным инновационным изменениям методов управления и технологий в целях повышения эффективности социально-экономических процессов [50].

С технологической точки зрения цифровая экономика представляет собой результат взаимного наложения фундаментальных прорывов в развитии нескольких отраслей деятельности, в том числе: создание кибер-физических и кибер-биологических систем, принципиально новых материалов, новых средств производства, ИТ, возобновляемых источников энергии и др. Переход к цифровой экономике характеризуется технологическими взрывами, под которыми понимается комбинация технологий, дающая возможность создавать новые продукты и сервисы, которые, с одной стороны, создают и формируют новые сферы деятельности, а с другой – уничтожают или радикально изменяют существующие отрасли экономики [64].

Техническое развитие носит экспоненциальный характер: каждый год новые наукоемкие технологии становятся все совершеннее, а их физическое воплощение все качественнее (материальные носители

информации становятся меньше по размеру и дешевеют, а их емкость и скорость обработки информации повышаются в разы) [111, с. 16].

Цифровую экономику правомерно рассматривать как составную часть шестого технологического уклада и четвертой промышленной революции, что объясняется следующими соображениями. Трансформация социально-экономических отношений, связанная с цифровой экономикой, разными научными школами трактуется по-разному. Наиболее распространенным является технологический подход, неразрывно связывающий развитие человеческой цивилизации с прогрессом технологий.

Его современный этап, именуемый в США, ЕС и других технологически развитых державах четвертой индустриальной (промышленной, технологической) революцией, в странах ЕАЭС отождествляется со становлением шестого технологического уклада.

Четвертая промышленная революция рассматривается как новый уровень организации и менеджмента цепочки создания стоимости на протяжении всего жизненного цикла выпускаемой продукции, то есть это концепция развития и интеграции технологий и подходов к повышению эффективности производства. В основу этого понятия положены следующие суждения:

1) переход от простой цифровизации (третья промышленная революция) к инновациям, базирующимся на интеграции технологий (четвертая промышленная революция), что вынуждает компании пересмотреть свое отношение к тому, как они работают [71];

2) все большее сближение физического, цифрового и биологического миров, что приводит к новым технологиям и платформам и созданию кибер-физических систем;

3) развитие интернета услуг, которые предлагаются как в пределах организации, так и между компаниями и используются участниками цепочки создания стоимости. То есть новые технологии позволили найти новые пути доставки товаров потребителю, что разрушило или изменило существующие до того каналы снабжения. Так, генерируемый в социальных сетях контент все активнее используется бизнесом для совершенствования моделей доступа к покупателю, для администрирования уличного трафика или борьбы с преступностью, энергетической и экологической оптимизации [34, с. 13];

4) усиление прозрачности в отношениях населения и власти, а также в деятельности властных структур, приводящее к децентрализации и перераспределению государственной власти. Мир становится постепенно прозрачным, что трансформирует характер

взаимоотношений между его участниками, изменяя, в том числе, существующий государственный механизм регулирования и управления;

5) кардинальная трансформация мирового сообщества, включая социальную, экономическую и политическую сферы; изменение положения человека в мире, перестройка его внутреннего мира, взаимоотношений в семье и с обществом, преобразование привычного уклада жизни, быта, семьи, жизненной среды, социально-экономических процессов в обществе, системы экономических отношений собственности, как в свое время мир преобразовали первые три промышленных революции [3].

Таким образом, закономерен вывод о четко прослеживающейся взаимосвязи и сопоставимости двух концепций: технологических укладов и промышленных революций (Таблица 4). Используя периодизации Львова-Глазьева и Шваба, место цифровой экономики на временной шкале 2010-2060 гг., она органически «вписывается» в заключительную фазу шестого технологического уклада или эпоху четвертой промышленной революции.

Профессор В. Ф. Байнев обращает внимание на то, что на начальном этапе четвертой промышленной революции, «…во-первых, телекоммуникационные и информационные технологии отнюдь не подменяют собой и не отменяют промышленные и другие традиционные производства, а обогащают их принципиально новыми возможностями, повышая экономическую эффективность и облегчая инновационную деятельность предприятий. Во-вторых, материальной основой всех нововведений в рамках четвертой промышленной революции опять-таки является продукция промышленности – микропроцессоры, микроконтроллеры, устройства передачи информации, цифровые исполнительные механизмы и т. д. И наконец, в-третьих, тот факт, что в основу периодизации эволюции технико-технологического прогресса на Западе положен именно промышленный фактор (Таблица 4), свидетельствует о понимании в странах-лидерах мирового хозяйства исключительной значимости индустриально-промышленного комплекса. Иными словами, именно промышленность, будучи главным производителем и поставщиком прогрессивных орудий труда и предметов потребления для прочих отраслей и сфер жизнедеятельности современного общества, является подлинным катализатором инноваций и локомотивом экономического развития в XXI в.» [11, с. 5].

***Таблица 4***

**Технологические уклады и промышленные революции**

| Технологический уклад | Промышленная революция | Основной источник роста | Среднегодовой рост совокупной факторной производительности, % |
|---|---|---|---|
| I | 1770-1840гг. (1-я промышленная революция – эпоха прядильного производства и пара | паровая машина, прядильная и ткацкая машины, металлургия, токарный станок | ≈ 1,5–2,0 |
| II | 1860-1900гг. (2-я промышленная революция – эпоха поточных производств и стали | телеграф, железные дороги, двигатель внутреннего сгорания, конвейер | |
| III | 1900-1910гг. (эпоха электричества) | черная металлургия, машиностроение, неорганическая химия, электричество, автомобилестроение | ≈ 1,0 |
| | 1920-е гг. (эпоха электричества) | | ≈ 2,0 |
| IV | 1930-е гг. (эпоха нефти) | производство и переработка нефти и газа, органическая химия, авиастроение, двигатель внутреннего сгорания | ≈ 3,0 |
| | 1940-е гг. (эпоха нефти) | | ≈ 2,5 |
| | 1950-1970гг. (3-я промышленная революция – эпоха автоматизации | компьютеры, микроэлектроника, атомная энергетика, роботы | ≈ 2,0 |
| V | 1970-2010гг. (эпоха ПК и интернета | | ≈ 1,5 |

| | | | |
|---|---|---|---|
| VI | 2010-2060-е (4-я промышленная революция – эпоха цифровой экономики | NBIC-технологии, генная инженерия, 3D-принтеры, ВИЭ, дроны, интернет вещей | – |

Можно полагать, что именно цифровые технологии, появившиеся более 50-ти лет назад, в условиях цифровой экономики, ставшие более усовершенствованными и интегрированными, распространяющиеся значительно быстрее и куда более масштабнее, вызвали смену технологического уклада и очередную промышленную революцию. По мнению многих экспертов, речь идет об изменении парадигмы экономического развития – цифровой революции, сопоставимой по значимости с аграрной, промышленной и научно-технической революциями (см. три «волны» в развитии общества Э. Тоффлера [107]). В данном контексте использование термина «революция» говорит не о скачкообразном характере изменений (которые, в отличие от революций политических, во всех четырех случаях носят накапливающийся характер постепенного перехода количества в качество), а об их радикальности – формировании новой модели хозяйственного устройства общества.

Смена парадигмы экономического развития характеризуется прежде всего изменением характера разделения труда. Так, аграрная (неолитическая) хозяйственная революция (ок. 8 тыс. лет до н. э.), повлекшая за собой переход человеческих общин от примитивной экономики охотников и собирателей к сельскому хозяйству (в марксистской историографии – от присваивающей к производящей экономике), связана с разделением сообщества на земледельцев, скотоводов, охотников, воинов, а также занятых в домашнем хозяйстве [111, с. 19].

Первая промышленная (Великая индустриальная) революция XVIII- XIX вв. характеризуется не только переходом от ручного труда к машинному, формированием промышленности как самостоятельной сферы производства. Одновременно преимущественно натуральное хозяйство, при котором большая часть продукции производилась для удовлетворения собственных потребностей, уступило место рыночной экономике, где блага производятся преимущественно для обмена, а целью функционирования хозяйствующих субъектов стало получение прибыли.

Третья промышленная революция (НТР), начавшаяся в середине XX в. как коренная перестройка материально-технической базы

общественного производства на основе комплексной автоматизации производства и управления, использования искусственных конструкционных материалов и новых видов энергетики, превратила в ведущий фактор производства науку, в результате чего началась трансформация индустриального общества в постиндустриальное. В наиболее развитых странах НТР обусловила стремительное развитие сферы услуг при значительном сокращении добычи природных ресурсов, производства промышленных товаров и сельскохозяйственного сектора.

Наконец, четвертая (цифровая) революция начала XXI в. Знаменует собой отделение центров разработки от производственных и обслуживающих подразделений, перераспределение большей части создаваемого общественного богатства в сферу интеллектуальной и организационной деятельности. В отличие от промышленной революции, происходит обратный процесс: индивидуализация продукции и возвращение производства значительной части потребительских благ и услуг в рамки домашних хозяйств на основе совершенствования бытовой техники, в ближайшем будущем – самостоятельное производство многих товаров в домашних условиях посредством 3D-принтеров. За счет компьютеризации и автоматизации подавляющей части операций, в том числе связанных с принятием решений, происходит вытеснение живого труда роботизированными комплексами и системами искусственного интеллекта.

В результате промышленных революций происходит также изменение способов выстраивания отношений между субъектами хозяйственной деятельности. В экономиках общинного типа преобладает механизм взаимного согласования (совещательная координация), в экономиках иерархического типа (феодальное и плановое хозяйство) – административный способ координации. В результате промышленной революции основным способом координации хозяйственного взаимодействия становится рыночный, предполагающий, что взаимодействие экономических агентов регулируется механизмом свободного ценообразования на основе конкуренции независимых продавцов и покупателей, стремящихся к максимизации собственной выгоды. Однако практически всегда и везде оно дополняется стандартизацией, административным регулированием и взаимным согласованием [78].

Итогом цифровой революции становится постепенное вытеснение рынка и переход к сетевым формам хозяйственного взаимодействия, в основе которых лежит формирование устойчивых связей между хозяйствующими субъектами на базе постоянного прямого

обмена информацией и выстраивания отношений взаимного доверия между очень широким кругом лиц.

## 1.3. Закономерности развития цифровой экономики

Трансформация национальных экономик в направлении бурного развития цифровой формы проявления новой экономики является актуальной гипотезой для развертывания как теоретических исследований и дискуссий в этой области, так и практических программных действий высших органов управления, направленных на создание техноцифровой платформы развития российской экономики.

Сущностная сторона цифровой экономики, как и новой экономики тесно связана с революционными изменениями в цифровой технологии, созданием и бурным развитием Интернета, инновациями, как в области Hard Ware, так и Soft Ware. Содержательная сторона цифровой экономики является многокачественной, и в первую очередь, за счет расширения многообразия форм проявления и развития «цифровизации» всех сторон жизни человека, богаче и разнообразней, чем сущностная определенность цифровой экономики и связана с технологическими, продуктовыми и сервисными инновациями [117]. Например, появление такой инновации, как компьютеризация промышленного дизайна и моделирования конструкторской подготовки производства существенно сокращает цикл разработки и проектирования продуктов высокой сложности, например, станков, автомобилей, поездов, самолетов, зданий и т. д.

В настоящее время многие специалисты и экономисты за рубежом и в нашей стране пытаются осмыслить и дать исчерпывающую характеристику современного состояния развития новой экономики, включая одну из форм ее проявления – цифровую экономику. Большинство исследователей через призму субъективного отношения выделяют как общее – объективное, присущее современной экономике, так и субъективное – собственное восприятие и понимание этого явления. Субъективно то, что экономисты стремятся уловить новые признаки в экономике и быстрее их описать, используя собственную терминологию и совокупность понятий, являющихся очень часто, при пристальном рассмотрении, синонимами. Объективно же это связано в большей мере с явным проявлением новых черт, сторон, признаков, тенденций и закономерностей в современной экономике. Изучение и учет новых экономических проявлений и, в частности, выделение

цифровой экономики как относительно самостоятельной части новой экономики представляет большой интерес, поскольку позволяет повысить скорость и качество управления экономикой, скорректировать правовое поле и правила ведения бизнеса, генерировать инновационные продукты, сервисы и услуги на основе цифровых технологий, включая новые экономические сферы – экономику впечатлений, MICE-индустрию, Smart-город и т. д.

Уделяя более пристальное внимание анализу новых явлений и тенденций в экономике, опираясь на работы американских исследователей таких как, например, Nicholas Negroponte, Chris Meyer, Mohanbir Sawhney, Daniel Spulber, Don Tapscott, Steve Jurvetson, Patricia Seybold и др., можно обнаружить стремление авторов охарактеризовать новые черты современной экономики, используя такие термины, как «новая экономика» (New Economy), «экономика 2000», «интернет-экономика» (Internet Economy), «Net экономика», «Web экономика», «цифровая экономика», «электронная коммерция» (E-economy, E-business), «нематериальная экономика», «невещественная экономика» и т.п. Данные термины часто используются как синонимы при рассмотрении новых явлений в экономике, обусловленных формированием глобальной электронной сети (Network), глобальным распространением ПК (PC), созданием и непрерывным совершенствованием программного обеспечения (Software), развитием ИТ, производством невещественных продуктов и услуг IT-компаний.

Опираясь на имеющиеся результаты исследований в данной области, можно предложить следующее определение предметной области цифровой экономики: цифровая экономика – это системная совокупность экономических отношений по поводу производства, распределения, обмена и потребления товаров и услуг техноцифровой формы существования. Техноцифровая природа экономических отношений являются ключевыми отличительными признаками цифровой экономики.

Таким образом, если новая экономика – это закономерная форма проявления постиндустриальной экономики, то цифровая экономика – это одна из эволюционных форм проявления новой экономики. Следовательно, как «форма формы» цифровая экономика содержит не только набор признаков новой экономики, но и содержит ряд отличительных сторон, характеризующих качественную определенность цифровой экономики [120].

Наряду с появлением новых закономерностей и тенденций, не имевших место в «индустриальной» экономике, обращает на себя

внимание новое содержание традиционных экономических постулатов, которые в сочетании и взаимосвязи с цифровыми технологиями проявляют себя по-новому. Под влиянием НТР, происходят существенные изменения в, казалось бы, канонических правилах рыночной экономики, правилах ведения бизнеса, в новых проявлениях традиционных экономических принципов и закономерностей [124]. Например, появление и развитие мировых электронных сетей, компьютеров и программных продуктов, цифровых технологий, электронных продуктов и услуг радикальным образом изменяет содержание, соотношение и значение в новой экономике следующих понятий: материального (вещественного) и нематериального (невещественного), географии и расстояния, пространства и времени, потребительной стоимости (полезности) и стоимости, количества и качества, конкуренции и потребительского предпочтения, посредничества и логистики, человеческого капитала и этики бизнеса, сделок и оценки эффективности, поведения продавцов и покупателей, новых отношений производителей и потребителей, технологий маркетинга и продаж и т.д.

Вполне очевидно, что по мере создания и бурного развития интернет-компаний и интернет-фирм в развитых странах и, в особенности в США, формируется новый рынок интернет-услуг, продуктов, сервисов, услуг провайдеров и т.п., проникающих во все сферы экономики и видоизменяющих экономику в целом. Поэтому целесообразно различать, на наш взгляд, интернет-экономику и цифровую экономику в узком смысле слова – как совокупность отношений по поводу создания и использования цифровых технологий, продуктов и услуг интернет-компаний и фирм, и в широком – новую экономику, экономику предприятий любых отраслей, функционирующую в условиях глобальной электронной сети с использованием цифрового формата технологий, и обладающую рядом отличительных признаков по сравнению с так называемой «индустриальной» экономикой, преимущественно соответствующей 3-му, 4-му технологическому укладу. Новая экономика в своем цифровом содержании характеризует более глубокий этап экономического развития общества на основе достижений 5-го и 6-го технологического укладов, когда индивидуалы и компании всего мира могут быть связаны между собой в самых многообразных сочетаниях благодаря Network и вступают в бизнес-отношения с использованием цифровых технологий практически мгновенно и независимо от посредников, расстояния или географического положения рынков, включая рынки инновационных цифровых технологий, продуктов, сервисов и услуг.

Таким образом, развитие цифровой экономики определяется, в первую очередь, не только революционными технологическими изменениями, но и закономерностями эволюции новой экономики в целом, ориентирует современный менеджмент на учет новых принципов управления и правил ведения бизнеса, способствует росту производительности труда и качества продукции, нивелирует отрицательные фазы экономического цикла, снижает инфляцию и безработицу, и в целом обеспечивает устойчивый рост экономики в условиях глобализации.

Глобализация экономических процессов становится основополагающей тенденцией и принципом развития современной экономики благодаря усилению интеграции различных сфер экономики, связанной с формированием мировой электронной сети. Данная закономерность новой экономики обеспечивает широкие возможности глобального бизнеса, с одной стороны, но и повышает ответственность фирм и компаний перед потребителями кардинальным образом, – с другой. Неудовлетворенность потребителей становится достоянием гласности практически мгновенно и очень широко [53].

Глобализация экономики, «исчезновение» материального и пространства в цифровой экономике приводит к изменению значения многих факторов производства и, в первую очередь, фактора времени. Время, как категория общественного производства, всегда определяло стоимостную оценку производства. Однако в современных условиях «цена» времени несоизмеримо возрастает. В мире «мгновенных» связей производителей и потребителей, время (его экономия и скорость сделок) являются большим, можно сказать стратегическим, преимуществом и одновременно критической ответственностью на любых рынках. Способность фирмы изучать ситуацию на рынке, оценивать условия для сделок, принимать решения и осуществлять сделки в режиме «online» – режиме реального времени, определяет ее успех или неудачу в мире бизнеса. К преуспевающим компаниям в этих условиях надо относить те (даже по сравнению с экономически сильными), которые проводят политику постоянных, непрерывных изменений к улучшению в производстве продукции, в первую очередь за счет цифровых технологий бизнеса и продвижения продуктов к потребителю. Такая политика позволяет ускорять «цифровизацию» НТП и обеспечивать стратегическое преимущество над внешне успешными традиционными компаниями.

Для новой и особенно для цифровой экономики характерно также быстрое изменение материально-вещественных факторов

общественного производства, как по форме, так и по содержанию, т. е. в сторону уменьшения их значения и физического содержания. Например, материалоемкость продукции и производства только за последние десятилетия в экономике развитых стран значительно снизилась. Если оценивать единицу физического веса валового внутреннего продукта за этот период в стоимостной форме, то можно обнаружить, что стоимость одного фунта продукции выросла за этот же период почти в 2 раза за счет информационно-цифровых факторов производства. Поэтому одной из ведущих тенденций цифровой и новой экономики принято считать «исчезновение» материального, замена материального на невещественные составляющие производства и продукции. Здесь имеется виду, прежде всего, тенденция возрастания роли и значения информационно-цифровой составляющей в затратах на производство: самой информации, цифровых технологий, интернет-услуг и сервисов, программных продуктов и т.д., по сравнению с материальной составляющей.

Процесс информатизации и цифровизации общественного производства является всеобщей тенденцией, но не является самоцелью, он ускоряется благодаря высокой экономической эффективности. Получение, цифровая обработка и передача информации все чаще становятся важнее физического, аналогового перемещения продуктов и даже иногда важнее самих традиционных денег. Кроме того, ценность компаний и фирм, их конкурентоспособность все в большей мере определяются не только материальным имуществом, а скорее нематериальным: знаниями людей, человеческим капиталом, идеями, искусственным интеллектом и стратегической совокупностью ключевой интеллектуальной собственности (обладанием идеями, инновационными цифровыми технологиями), обеспечивающими стратегическое превосходство фирмы над конкурентами.

В условиях цифровой экономики роль расстояния и географического местоположения производителей и потребителей существенно уменьшается. Пространство как бы «исчезает», продавцы и покупатели в сетях не чувствуют расстояний. Весь мир превращается в глобального, но конкретного потребителя и конкурента одновременно. Раньше географическое положение и расстояние играли гораздо большую роль в конкуренции. Сейчас любой бизнес может быть связан немедленно (практически мгновенно) и глобально со всеми потребителями при помощи мировой электронной сети и услуг интернет фирм и, с другой стороны, ни один производитель в этих условиях не защищен от

конкурентов и может быть вытеснен, устранен на рынке одним движением компьютерной «мыши».

Следует отметить, что генерирование и взаимосвязь всего нового в экономике по-прежнему обеспечивается человеком [129]. Умственный потенциал людей и сила интеллекта никогда не могут быть окончательно высокими (включая технологии искусственного интеллекта), не имеют предела, обусловливают прогресс в любой области. Поэтому человеческий капитал, интеллект работников становится ведущим фактором новой, цифровой экономики. Если современные традиционные технологии в условиях рынка доступны практически всем фирмам, то новые цифровые технологии бизнеса и привлечения потребителей какое-то время целиком относятся к «ноу-хау» персонала фирм и компаний. Все большие объемы национального богатства и общественных ценностей обеспечиваются смелыми идеями и решениями в области передовых технологий производства и новых моделей бизнеса. Люди, способные работать творчески, инновационно и на основе цифровых технологий являются практически бесценными. Это ведет, в свою очередь, к изменению, развитию методов управления персоналом на предприятиях и фирмах, направленных на максимальное использование человеческого потенциала [101].

Совокупный человеческий капитал (рабочая сила) в цифровой экономике становится более мобильным и гибким, что позволяет работодателям довольно часто обходить дорогостоящие рынки организованной рабочей силы (в виде общественных организаций и профессиональных союзов) и действовать напрямую с каждым работником (через Big Data и персональные данные о качестве рабочей силы). Этоповышает скорость движения рабочей силы и снижает удельные затраты по оплате человеческого капитала [94]. Относительное сдерживание роста заработной платы по сравнению с ростом производительности труда обеспечивается снижением степени гарантий занятости за счет глобальности и гибкости рынка рабочей силы. Работники, со своей стороны, в условиях цифровой экономики предпочитают выбирать стабильную занятость в сравнении с активностью по повышению заработной платы. При прочих равных условиях достигается определенный компромисс в поведении работодателей и работников.

Другой особенностью цифровой экономики следует считать принцип ускорения экономического роста. Благодаря Network (электронной сети) значительно ускоряется распространение и адаптация продукции в сфере обращения и потребления. Электронная сеть и цифровые технологии делают сетевой маркетинг более эффективным:

информация о продуктах, ситуациях на рынках распространяется по принципу цепной реакции. Согласно этому положению, первое решение и правильное действие часто обеспечивают большие преимущества и получение дополнительной выгоды. Хорошие, качественные товары распространяются и продаются в режиме «online» со скоростью, сравнимой с распространением вируса в живой природе. «Вирусный» маркетинг обеспечивает ускорение экономического роста любой фирмы. Примером могут служить многие интернет-компании различных стран, занимающиеся электронной коммерцией и Интернет-торговлей.

Создание новых цифровых ценностей и, следовательно, добавленной стоимости через деятельность каждой интернет-компании обусловливает повсеместность роста общественного богатства. Создание ценностей, в свою очередь, зависит от деления существующих рынков. Современные компании все чаще продвигают даже известный продукт с целью обеспечения доли рынка и затем развивают продажу связанных с ним новых услуг и товаров через использование сетей. Зависимость ценности продукта от доли рынка обусловливается широкомасштабным развитием электронной сети. Если раньше ценность продукта во многом определялась его дефицитностью, то сейчас, благодаря Network, исключение быстро превращается в правило, цена товара снижается. По видам продуктов, которые помогают устанавливать «стандарты» потребления, эффект от продаж изменяется по степенной функции в зависимости от доли рынка. В условиях цифровой экономики через сеть можно найти практически все: товары, услуги и любую информацию, которая нужна потребителю. Более того, новые пользователи могут вести свою экономическую политику и добавлять информацию с целью дальнейшего деления и завоевания рынка. Эффективность компаний, работающих в режиме «online» обеспечивается, в первую очередь, настойчивостью, мобильностью, коммуникабельностью персонала, коллегиальностью принимаемых решений и индивидуальным подходом к пользователям сетей (потенциальным покупателям) на основе технологий Big Data.

Для цифровой экономики характерно также изменение института посредничества. Деятельность посредников сейчас видоизменяется, поскольку информированность и осведомленность покупателей заменяется прямой взаимосвязанностью участников рынка. С одной стороны, традиционные дистрибьюторы и агенты в развитых странах сталкиваются в настоящее время с серьезными трудностями в своей работе в связи с развитием интернет-сети, в которой покупатели и

продавцы связаны напрямую и обходятся без посредников в своих сделках. С другой стороны, количество информации растет стремительно и пользователи (покупатели) остро нуждаются в своеобразных «фильтрах», отсеивающих ненужную информацию. В этих условиях создаются предпосылки возникновения нового типа посредничества – информационного посредничества (инфопосредничества). Все чаще появляются инфоинтернет-компании, предлагающие агрегированные услуги или интеллектуальное обслуживание потребителей, направленные на сильную и технологически обеспеченную помощь в осуществлении сделок во всех аспектах. Эти компании формируют так называемую коммуникативно-организованную среду для удобства потребителей и для блага, естественно, собственного бизнеса. Инфопосредники организуют продавцов и покупателей, определенным образом связывая их, с учетом взаимных интересов через электронные сети и на основе цифровых технологий. Интересно, что инфопосредниками могут стать любые компании, имеющие частые контакты со всеми участниками рынка и обладающие соответствующим цифровыми технологиями, а также потенциальной полезной информацией об этих участниках из формируемых баз данных.

С появлением глобальной электронной сети покупатели получили новые беспрецедентные возможности удовлетворения своих потребностей, а продавцы, в свою очередь, новый источник своей экономической силы (потенциала) для роста. В условиях цифровой экономики уже нет необходимости «физического» изучения цен и условий продаж на рынках, аналогового сравнения цен в различных магазинах и фирмах. Альтернатива определяется быстро одновременно с обследованиями, а конкурент может быть устранен одним движением компьютерной «мыши». Программные системы (Software) и сервисы интернет-фирм помогают покупателям найти лучшие варианты. Поэтому продавцы и бизнесмены предлагают либо действительно уникальные высококачественные товары и сопутствующие услуги, либо меньшие цены и затраты при прочих равных условиях. Процветание компаний при этом зависит от прибыли, получаемой от притока новых покупателей и, следовательно, от их умения работать в «цифровом формате» и сетях. Принцип физической конкуренции заменяется на принцип «виртуальной», но не менее жесткой от этого, конкуренции на рынках цифровой экономики. Специфика данных рынков заключается в том, что цены на продукты и услуги на них отражают все изменения (факторы) во взаимосвязи и практически в реальном времени.

Важным аспектом интернет-экономики и цифровой экономики, в частности, является особая технология ведения бизнеса. Особенность заключается в том, что сделка осуществляется по принципу «один на один» и без участия традиционных посредников, либо с участием инфопосредников. Поэтому информационная составляющая стоимости товара, услуг становится все большей. При этом продавцы находят этот процесс более рентабельным, так как стоимость цифровизации является более эффективной, чем осуществление затрат на традиционные составляющие стоимости товара. Потребители, в свою очередь, стремятся индивидуализировать свои требования к продукту в соответствии с их желаниями. Возникают беспрецедентные условия информационного обмена между поставщиками и потребителями, между продавцами и покупателями. И для тех, и для других информация является ключевым моментом их экономической жизни.

Достаточно новым положением новой цифровой экономики можно считать слияние маркетинга и процесса купли-продажи в единый процесс. Благодаря «World Wide Web (w.w.w.), - системы, практически не имеющей ограничений, каждый продукт становится доступным везде, где имеется сеть и организована электронная коммерция. Разрыв между желанием и покупкой в режиме «online» исчезает: поиск желаемого товара и его покупка не разделяются физическими барьерами или чувственными восприятиями, они сливаются в условиях цифровой экономики в единый процесс.

Цифровая технологическая платформа (техноцифровой базис новой экономики) дает уникальные возможности для реализации методологии селективно-адресного взаимодействия социально-экономических субъектов. Формирование баз данных, больших таблиц или больших массивов данных (Big Data) в купе с появлением новых цифровых технологий работы с информацией на суперкомпьютерах позволяет определять предпочтения субъектов отношений и генерировать адресные воздействия и предложения каждому индивиду. Индивидуальный подход к каждому потребителю или участнику отношений (в том числе и социально-политических) в условиях глобализации отношений, благодаря «цифре», становится реальностью и эффективным инструментом управления.

Некоторые специалисты, например, Алан Гринспен, отмечают, что по мере развития цифровой экономики и, следовательно, более активного действия факторов роста производительности труда и снижения уровня безработицы видоизменяется характер цикличности экономики. Цикличность цифровой экономики не исчезает, но цикл

сглаживается за счет уменьшения действия факторов, вызывающих спад экономики.

Цифровизация контроля запасов, затрат на рабочую силу и логистику позволяет минимизировать затраты на готовую продукцию и контролировать, в конечном счете, рост цен (например: система снабжения «канбан» -«точно в срок», штрихкодирование и сканирование информации, GPS-контроль транспорта, вертикальное связывание услуг, уменьшение резерва рабочей силы). Другие исследователи, такие как Майкл Мэндел, считают, что экономический цикл в цифровой экономике зависит от технологического цикла, который, несмотря на развитие высоких технологий, ведет к неустойчивости экономики и затем к кризису.

Принимая во внимание основные закономерности развития цифровой экономики можно выделить главные принципы ее функционирования и, следовательно, учитывать их при совершенствовании управления цифровой экономикой. К ним относятся следующие принципы.

1. Принцип «исчезновения» материально-вещественной составляющей и замены ее «нематериальной» компонентной: человеческим капиталом, идеями, знаниями, искусственным интеллектом, Soft Ware и т. д. При этом скорость «исчезновения» материальности увеличивается, а эффективность цифровой экономики повышается пропорционально росту «невещественной» составляющей.

2. Принцип «сжатия» пространства и уменьшения значения расстояния в условиях глобализации цифровой экономики – важнейший принцип современной экономики. Глобальность цифровой экономики объединяет производителей, потребителей и конкурентов вне зависимости от географической локализации. Все связаны со всеми и не «защищены» друг от друга в плане ответственности и конкурентоспособности своего бизнеса. Географическое положение в конкуренции не имеет уже такого важного значения в цифровой экономике, как в прежней «доцифровой» экономике.

3. Принцип «сжатия» времени означает повышение скорости всех экономических отношений, изменений и, что особенно важно, принятия управленческих решений. В условиях быстрых связей в общественном производстве время становится большим преимуществом и ответственностью одновременно. Цифровые компании обеспечивают большую экономию рабочего времени по сравнению с традиционными компаниями. Стратегия цифровых компаний направлена на

постоянные изменения по всему производственному циклу, а ускорение изменений по улучшению обеспечивает им конкурентные преимущества.

4. Принцип «smart» организации и управления является не менее важным в цифровой экономике. Человеческий капитал, люди, знания, идеи, искусственный интеллект – это ведущая ценность цифровой экономики [90]. Она обеспечивает содержание и скорость изменений в технологической сфере, появление смелых идей и инноваций в бизнесе и управлении. Человеческий капитал становится «бесценным» в цифровой экономике, а управление персоналом направлено на способность компании генерировать «побеждающие» технологии и решения.

5. Принцип «сетевого» роста и развития в условиях цифровой экономики связан с особым, «вирусным» характером коммуникаций и, в первую очередь, благодаря электронной сети (Network). Легкость коммуникаций и их цепной характер способствуют быстрому распространению осведомленности всех участников бизнеса. Компании, работающие через Интернет, могут иметь взрывной рост продаж благодаря правильному первому шагу, правильной организации сетевого маркетинга. Использование цифровых технологий в мире пользователей Интернетом, итерационное планирование и управление могут способствовать ускорению экономического роста при прочих равных условиях.

6. Принцип ценности технологических платформ (включая цифровые формы) и стандартов обусловлен быстрым распространением удачных единичных решений, которые превращаются затем в основу масштабного производства, в правило, обеспечивающее завоевывание большей доли рынка. В последующем с данной платформой связываются сопутствующие виды продукции и услуг. В цифровой экономике все чаще появляются event- комплексы продукции и услуг, определенных некоторым событием, формирующих образ и стиль жизни людей, которые становятся ведущими ценностями и стандартами потребительского поведения. Производители и продавцы не могут не замечать данные обстоятельства и учитывают их при организации бизнеса.

7. Принцип «эффективности» работы с информацией направляет участников (субъектов) цифровой экономики на упорядочение большого массива информации. Все участники нуждаются в «фильтрации» информации с целью выделения особо важной и полезной информации в каждом конкретном случае. Пользователи нуждаются в фильтрах, отсеивающих ненужную информацию. Поэтому появляется потребность в агрегированных услугах и «smart»-обслуживании клиентов. Часть

цифровых компаний специализируются на этом и превращаются в эффективных информационных посредников.

8. Принцип «виртуальности» рынка приводит к ненужности физического появления или присутствия на рынке. Сравнение цен и конкурентных преимуществ продукции можно делать, не заглядывая в торговые центры, а специальные программы могут обеспечить поиск продукции с оптимальным соотношением цены и качества. Физические барьеры в конкуренции исчезают, бизнес стремится предложить лучшее качество и меньшие цены, покупатель реагирует мгновенно: поиск и покупка происходят практически одновременно, без посещения торговых точек.

9. Принцип изменения структуры затрат в цифровой экономике имеет существенное значение. Информационная компонента в стоимости товара становится все большей, а материально-вещественная сторона – меньше. Эксплуатация или потребление высокотехнологичной продукции обходится потребителю (на единицу полезного эффекта) дешевле, доставляет большее удовлетворение и восхищение. Компании с высокой степенью инновационности также имеют преимущества за счет изменения структуры себестоимости производства и уменьшения транзакционных затрат.

10. Принцип «импульсной» мотивации означает, что выбор товара и покупка благодаря Интернету происходит часто импульсивно, как единый и мгновенный процесс. Появление желания и покупка происходят по время поиска другого товара. Пробела между поиском, желанием и покупкой практически нет. «Мягкое» принуждение к изменению выбора находится в арсенале цифровых компаний.

11. Принцип «интернационализации» цифровой экономики можно трактовать как проявление международного разделения труда с одной стороны, и развитие (глобализация) мировых экономических отношений – с другой. Глобализации экономики благодаря цифровым технологиям снимает барьеры и ограничения по производству и потреблению продукции. Логистика и торговля благодаря цифровизации делают товары доступнее и удобнее. Сопровождение всех этапов жизненного цикла продукции обеспечивается на различных языках, а существование специальных программ позволяет осуществлять перевод информации с одного языка на другой практически моментально и без переводчиков. Международная стандартизация и передвижение человеческого капитала также способствует интернационализации цифровой экономики.

Таким образом, современные тенденции развития мировой экономики во многом обусловлены и будут определяться в дальнейшем развитием глобальной электронной сети, информационно-интеллектуальными и цифровыми технологиями, более полной реализацией потенциала человеческого капитала и искусственного интеллекта. Поэтому изучение проблем цифровой экономики представляется весьма актуальным, как с точки зрения экономической науки, так и с позиций практической трансформации систем менеджмента различного уровня: от электронного правительства до цифровых моделей smart-управления различными объектами (городом, движением транспорта, домом, квартирой, автомобилем и т. п.). Необходимо также отметить, что важнейшим аспектом цифровизации общественной жизни, оставшимся за пределом данной главы, является проблематика экономической и компьютерной безопасности, приобретающая все большую актуальность по мере развития и становления цифровой экономики.

## 1.4. Тенденции развития «цифровой экономики» в России

В последние годы цифровая экономика динамично становится одной из самых влиятельных отраслей экономики Российской Федерации, что помогает достигать средних и высоких темпов экономического роста. Российское правительство придает огромное значение развитию цифровой Экономики [8].

Сегодня сектор высоких технологий в России составляет менее четверти всей экономики, что ставит ее на скромное 44-е место в мире. На Россию приходится менее 0,5% мирового экспорта высокотехнологичной продукции. Результаты деятельности информационной индустрии в значительной степени определяет сектор ИКТ: на него приходится 90% валовой добавленной стоимости и 87% занятых в этом сегменте экономики. В 2016 г. российский сектор ИКТ насчитывал 166 тыс. организаций с численностью занятых 1,4 млн человек. Вклад сектора ИКТ в экономику страны можно оценить по его доле в ВВП. В 2016 г. она составила 2,9%. Объем валовой добавленной стоимости в реальном выражении достиг 2265 млрд руб., прирост по сравнению с 2010 г. в постоянных ценах – 19% (в 2,7 раз выше, чем прирост ВВП), по сравнению с 2015 г. – снижение на 5%. [112]. Согласно данным РАЭК, в российской сфере ИКТ работают 2,5 млн человек (годом ранее было 2 млн человек).

Вместе с тем, официальная статистика свидетельствует, что российская экономика находится в начале пути к цифровизации. Так, доля продукции высокотехнологичных и наукоемких отраслей в валовом внутреннем продукте России не превышает 23%, также невелика доля инвестиций в основной капитал в структуре ВВП (Таблица 5).

Однако следует отметить положительную динамику инновационного развития высокотехнологичных отраслей, представленных такими видами деятельности как производство фармацевтической продукции, вычислительной техники, электронных компонентов, аппаратуры для радио, телевидения и связи, медицинских изделий, средств измерений, контроля, управления и испытаний, оптических приборов, фото и кинооборудования, часов, летательных аппаратов, включая космические (Рисунок 3). Также наблюдается положительная динамика изменения затрат на технологические, маркетинговые и организационные инновации (Рисунок 4).

***Таблица 5***

**Показатели эффективности российской экономики в 2012-2016 гг.**

| Показатель | 2012г. | 2013г. | 2014г. | 2015г. | 2016г. |
|---|---|---|---|---|---|
| Доля продукции высокотехнологичных и наукоемких отраслей в ВВП, в % к итогу | 20,3 | 21,1 | 21,8 | 21,5 | 22,4 |
| Доля инвестиций в основной капитал в ВВП, в текущих ценах, в % к итогу | 20,7 | 20,9 | 21,2 | 20,5 | 19,6 |
| Прирост высокопроизводительных рабочих мест, в % по отношению к предыдущему году | 12,7 | 6,9 | 4,5 | -9,1 | -4,8 |
| Степень износа основных фондов, в % | 47,9 | 47,7 | 48,2 | 49,4 | 47,7 |
| Инновационная активность организаций, % | 10,4 | 10,3 | 10,1 | 9,9 | 9,3 |
| Доля внутренних затрат на исследования и разработки в ВВП, % | 1,02 | 1,05 | 1,06 | 1,07 | 1,10 |
| Коэффициент изобретательской активности (число патентных заявок на изобретения, поданных в России, в расчете на 10 тыс. человек), единиц | 2,00 | 2,00 | 1,65 | 2,00 | 1,83 |

Источник: [112].

Для капиталоемких отраслей промышленности, таких как добыча нефти и газа, электроэнергетика, технологии «Индустрии 4.0» открывают возможности существенного повышения эффективности, но не влекут за собой радикальной трансформации бизнес-модели [14]. Для более трудоемких отраслей воздействие инструментов «Индустрии 4.0» заключено в повышении эффективности производственного процесса за счет автоматизации, использования подключенных к промышленному интернету вещей датчиков и углубленной аналитики.

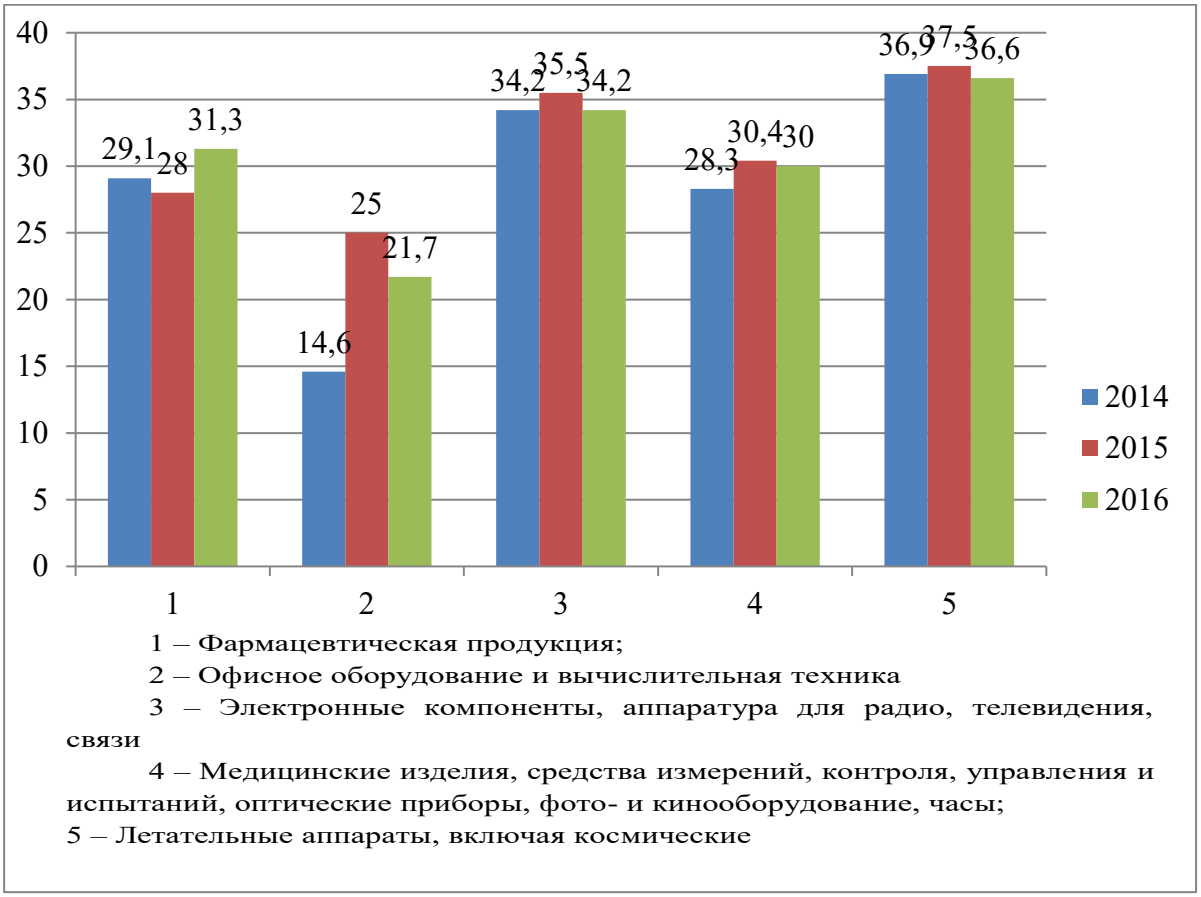



**Рисунок 3** – Инновационная активность организаций по видам экономической деятельности [112]


**Рисунок 4** – Затраты на технологические, маркетинговые, организационные инновации, в % к итогу [112]

Процент внутренних затрат на проведение научных исследований и разработок в организациях сектора ИКТ от ВВП имеет незначительную тенденцию роста. Оценивая количество организаций, проводящих в общем по НИОКР и количество занятых в них, можно констатировать, что за 20 лет они уменьшились в среднем на 20% (данные Росстата до 2014 года). Данная проблема возникла в последствии эмиграции высоквалифицированных молодых специалистов, так как в Российской Федерации тяжело продемонстрировать свой потенциал и добиться карьерного роста. В данной сфере стоит следующая задача – повышать эффективность, отдачу от исследовательских работ и разработок, и к тому же делать их конкурентоспособными на мировом рынке [103].

При этом Россия отстает от стран-лидеров цифровизации на 5–8 лет [23]. Если текущие темпы роста цифровой экономики России сохранятся на прежнем уровне, то к 2020 году, в силу высокой скорости глобальных изменений и инноваций, этот разрыв будет составлять уже 15–20 лет. Вместе с тем, в последние годы улучшилось состояние инфраструктуры в России, в первую очередь по уровню проникновения проводного интернета (74,8% от общей численности населения).

Сегодня Россия не входит в группу лидеров развития цифровой экономики по многим показателям – уровню цифровизации, доле цифровой экономики в ВВП, средней задержки в освоении технологий,

применяемых в странах-лидерах. Доля цифровой экономики в ВВП России составляет 3,9%, что в 2–3 раза ниже, чем у стран-лидеров, но заметен и ряд положительных тенденций [30].

Один из важнейших показателей – объем цифровой экономики – в последние годы стремительно растет. В России практически с нуля удалось создать крупные цифровые компании, и некоторые из них добились международной известности. Это крупнейший в мире независимый онлайн-банк «Тинькофф Банк», который не имеет физических отделений, цифровые порталы и экосистемы сервисов «Яндекс» и Mail.ru, производитель морских тренажеров и электронных навигационных систем «Транзас», площадка электронных объявлений Avito, социальная сеть «ВКонтакте», компания по производству цифровых решений в области безопасности «Лаборатория Касперского» и многие другие.

В 2015 году в отчете McKinsey «Эффективная Россия: производительность как фундамент роста» указывалось на то, что основой дальнейшего экономического роста страны станет повышение производительности трудовых ресурсов и капитала. Цифровая экономика в настоящее время является основой экономического развития страны.

Ниже представлено (Рисунок 5) развитие цифровой трансформации экономики в России с 1997 по нынешнее время. В 1997 году произошел первый этап оптимизации бизнес-процессов, 2007 году дальнейшая автоматизация процессов, а также улучшение подготовки кадров. В 2016 г. в России развивается Индустрия 4.0. и происходит цифровизация, развивается современная система образования поскольку цифровая экономика «требует» «цифровых» навыков [134].


**Рисунок 5** – Цифровая трансформация экономики

Цифровая экономика России получила значительный импульс развития за последние годы. Определенных успехов достигли частные компании, преобразуется рынок труда, при поддержке государства реализуются беспрецедентные инфраструктурные проекты, повышающие уровень доступности цифровых услуг для населения и бизнеса, широкое распространение получили интернет, мобильная и широкополосная связь [79].

В настоящее время достаточно сложно измерить эффективность цифровой экономики – отсутствует единый подход к измерению, методы расчета ключевых показателей могут быть неточными ввиду незрелости моделей и недостаточного анализа всех особенностей сферы цифровой экономики [55].

На графике ниже представлена тенденция развития цифровой экономики в России (Рисунок 6)

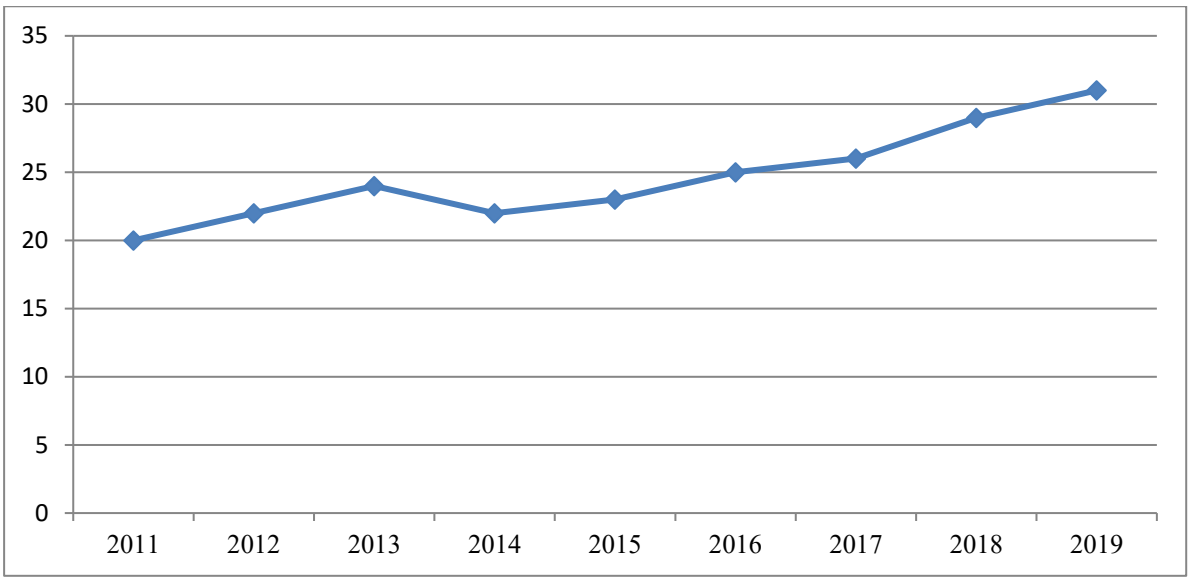



**Рисунок 6** – Тенденция развития цифровой экономики в России

Несмотря на это, сохраняется отставание от стран-цифровых лидеров по ключевым показателям развития цифровой экономики, в частности от Европейского союза [84]. (Рисунок 7).

На сегодняшний день значение ключевого для развития цифровой экономики показателя, как соотношение между объемом цифровой экономики и совокупным ВВП страны, составляет 3,9%, что примерно в 2–3 раза ниже, чем в выбранных для сравнения странах. Построение цифровой экономики в Российской Федерации, позволит получить ряд потенциальных преимуществ, к примеру, использование цифровых технологий, как в государственном секторе, так и в бизнесе. В РФ уже запущен портал www.gosuslugi.ru, с помощью которого значительно повысилась доступность различных государственных услуг, сократилось время на их получение. Также в России есть такие «цифровые гиганты», как «Яндекс», «Касперский», службы онлайн-заказов, которые также участвуют в диверсификации российской экономик. По данным рисунка 7 отмечен высокий показатель проникновения мобильной связи, которая включает в себя интернет-услугу. Кроме того, планируется, что уже к 2020 г. 95% населения Российской Федерации будут иметь доступ к интернету [2].

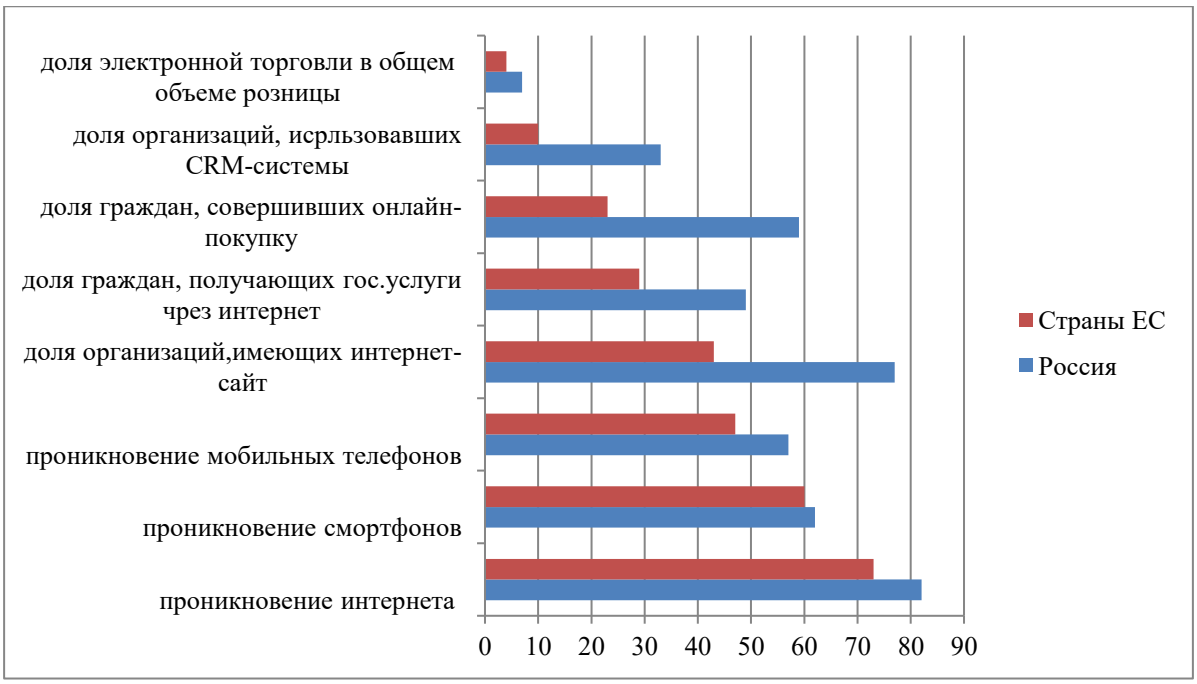



**Рисунок 7** – Доступ к цифровым сервисам в России и странах ЕС

Таким образом, уровень использования цифровых технологий оказывает значительное влияние на объемы ВВП стран уже на сегодняшний день, что было доказано с помощью проведенного регрессионного анализа и выявления тесной связи между глобальным индексом подключения и валовым продуктом на душу населения. При этом влияние данного фактора будет только усиливаться по мере развития инноваций в данной сфере ИТ во все сферы жизнедеятельности. Поэтому, несмотря на имеющиеся проблемы, государственный курс на внедрение и развитие цифровой экономики является единственным возможным путем укрепления стратегических позиций Российской Федерации в мировой экономике [29].

Сложная, но достижимая цель – утроение объема цифровой экономики с 3,2 трлн руб. в 2015 году до 9,6 трлн руб. в 2025 году, в ценах 2015 года (Рисунок 8), что потребует сохранения среднегодового темпа роста объемов цифровой экономики на уровне 12%, который наблюдался в 2010–2015 годах. Эти результаты будут эквивалентны увеличению доли цифровой экономики с текущих 3,9% до 8–10% ВВП (в зависимости от цен на нефть и других макроэкономических параметров), что в среднем соответствует сегодняшнему уровню стран, лидирующих по объему цифровой экономики: США, Китая и Западной Европы [95].

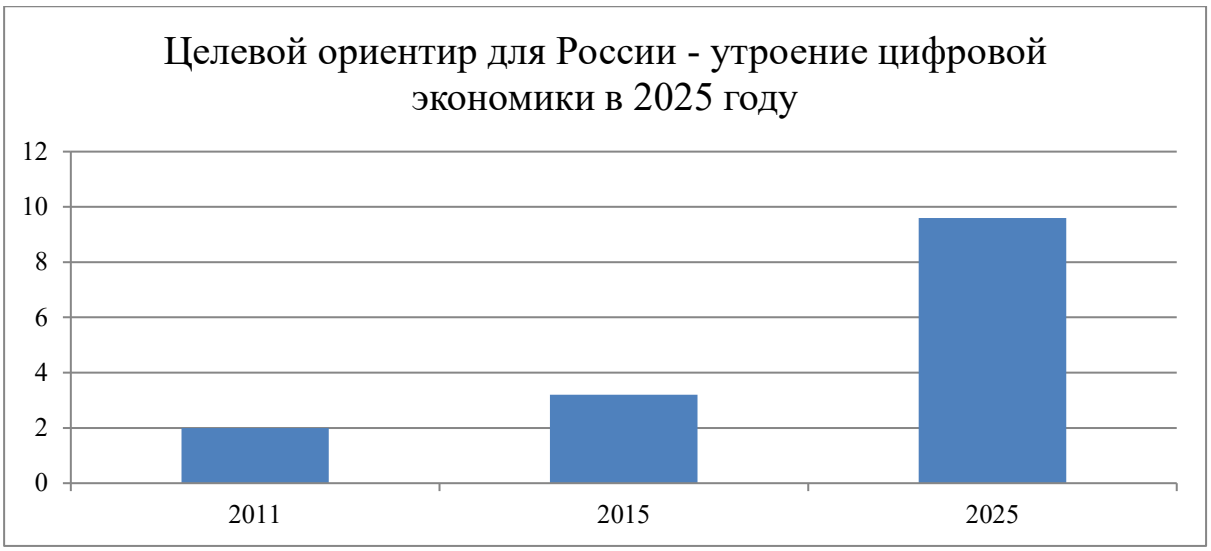



**Рисунок 8** – Прогноз: «Утроение цифровой экономики в России»

Интенсивное внедрение цифровых технологий значительно сократит отставание Российской Федерации от стран-лидеров, а также повысит долгосрочное устойчивое развитие. По прогнозу к 2020 году доля цифровой экономики в России возрастет. Такие экономические прогнозы связаны не только с эффектом от автоматизации существующих процессов, но и с внедрением принципиально новых, прорывных бизнес-моделей и технологий. Среди них – цифровые платформы, цифровые экосистемы, углубленная аналитика больших массивов данных, технологии «Индустрии 4.0», такие как 3D-печать, роботизация, интернет вещей [4].

По данным Рунета «Информатика и вычислительная техника» сегодня занимает 7 место в России в общем рейтинге специальностей. Ежегодно учреждения высшего образования России выпускают около 25 тысяч IT-специалистов, из которых лишь 15% готовы к немедленному трудоустройству и эффективной работе в отрасли. А средний срок адаптации сотрудника-выпускника на рабочем месте составляет от 0,5 до 1 года. Таким образом, дефицит квалифицированных трудовых ресурсов в сфере IT сохраняется и местами усиливается [100].

В 2011 году вклад цифровой экономики в ВВП России The Boston Consulting Group (BCG) оценивала в 1,6 % [4]. Исследование «Экономика Рунета», проведенное Российской ассоциацией электронных коммуникаций (РАЭК), цифровая экономика по итогам 2016 г. составляет 2,8% ВВП России или $75 млрд, в то время как в 2015 г. на нее приходилось 2,3% ВВП [5]. По данным BCG доля цифровой экономики в ВВП развитых стран – 5,5%, развивающихся – 4,9%. [99].

Главной проблемой развития цифровой экономики является низкая склонность предприятий к внедрению цифровых технологий, что, в свою очередь, приводит к снижению производительности труда и замедляет трансформацию традиционной экономики [28].

По мнению международной компании McKinsey, работающей в сфере управленческого консалтинга, источником долгосрочного экономического роста станет именно цифровизация российской экономики. Потенциальный эффект для ВВП от цифровизации экономики к 2025 году оценивается в 4,1–8,9 трлн. рублей, что составит 19–34% общего увеличения ВВП.

Исходя из вышеизложенного дальнейшая цифровизация экономики – неизбежна для Российской Федерации. Для ускоренного и эффективного развития цифровой экономики Российской Федерации необходимо: содействие в развитии ИКТ, где содержится основная часть кадров требуемых цифровой экономикой [56]; необходимо стимулировать масштабное внедрение инноваций и технологическую трансформацию в отраслях, особенно в промышленности [114]. В основе технологического развития предприятий будет лежать развитие глобальных промышленных сетей и соответствие требованиям «Индустрии 4.0»; государству необходимо оказать поддержку обществу на пути к освоению цифровых требований.

Таким образом, имеющиеся статистические данные свидетельствуют о наличии определенных препятствий в развитии цифровой экономики в Российский Федерации в части доступности информационно-коммуникационной энергетической инфраструктуры населению страны. Именно на преодоление этих трудностей и должны быть направлены усилия государственной власти в ближайшее время.

## 1.5. Подготовка кадров для цифровой экономики и проблемы труда в условиях цифровизации

Цифровые технологии стремительно входят в нашу жизнь, оказывая значительное влияние на формирование новых секторов экономики и предъявляя новые требования к структуре компетенций сотрудников, которые будут востребованы в условиях нового технологического уклада. Исследователи высказывают подчас противоречивые мнения относительно того, как цифровая трансформация повлияет на занятость населения в будущем и какие именно компетенции сотрудников будут востребованы. Согласно отчету BCG «Россия 2025: от кадров к талантам», представленному в 2017 году, «…в перспективе 10-20

лет исчезнут 9-50% ныне существующих профессий» [4]. Представленная картина во многом является пугающей, вносит хаос и оказывает деструктивное воздействие на решения, принимаемые экономическими субъектами. Однако, при более детальном анализе ситуации становится понятно, что через подобные трансформации рынка труда человечество проходило уже неоднократно и связанно это было с несколькими НТР, имевшими место ранее. Можно выдвинуть тезис, что, вычленив факторы, оказывающие влияние на развитие конкретной НТР, мы сможем определить ключевые компетенции сотрудников периода цифровой экономики.

В настоящее время лидерские позиции в использовании цифровых технологий занимают компании США. Им принадлежит огромное количество данных и новейших научных разработок в области построения многомерных моделей с использованием технологий Big Data, что формирует цифровое неравенство в мире [7].

В России только отдельные компании решаются на диджитализацию («Техносерв», «Технониколь», «Айтеко», «Сибинтек», «Revolta Engineering, Jandex Deite Factory). Это обусловлено не только технологическим и инфраструктурным отставанием РФ от промышленно развитых стран, но и значительным дефицитом специалистов в области цифровой экономики и цифровой культуры взаимодействия компаний с деловыми партнерами. Для решения этих задач необходимы большие объемы инвестиций, формируемые как за счет средств государства, так и частного бизнеса. В ВВП России доля цифровой экономики составляет 2,1% (в Великобритании – 8,4%, в США – 6%, в странах ЕС – в среднем 5%). По доле в ВВП расходов на науку Россия в 2015 г. находилась лишь на 34 месте в мире (1,12%). В США этот показатель составлял – 2,8%, в Японии – 3,6%, в среднем по ЕС – 2% [112]. К тому же доля затрат на образование в ВВП России составляет 4%, в то время как в СССР она составляла 10–12%.

Главной особенностью цифровой экономики являются знания. Чтобы занять достойное место в цифровизации России необходимо осуществить революционные изменения в науке и образовании. В «Программе развития цифровой экономики до 2025 г.» одним из важнейших направлений является «кадры и образование», так как невозможно осуществить революционные преобразования без кадровых изменений.

Эти изменения касаются в первую очередь управленческого персонала. Между тем существующий уровень осознания лидерами бизнеса и в целом менеджерского корпуса отечественных предприятий

предстоящих глубоких изменений и тем более готовности к ним крайне низок.

Именно человек является ключевым элементом механизма построения умного города, выступая и как созидатель его положительных сторон, и как их потребитель. Как созидатель человек разрабатывает концепцию построения умного города, определяет и мобилизует нужные для этого ресурсы, отслеживает и анализирует динамику развития данного процесса, при необходимости вносит соответствующие коррективы и дополнения, принимает технические и технологические решения. В качестве потребителя человек активно использует преимущества умного города, что облегчает и повышает качество его жизнедеятельности, позволяет ему экономить время и финансовые ресурсы.

В связи с этим образование является важнейшим источником формирования новой управленческой элиты, способной конкурировать в глобальной и цифровой экономиках. Именно человек с его знаниями, умениями и навыками является главным ресурсом цифровой экономики. Ценность данного ресурса зависит, прежде всего, от широты и глубины накопленных знаний.

Овладение новыми знаниями, с одной стороны, облегчается доступом к БМД, а с другой стороны, затрудняется рисками, связанными с выбором способов приобретения знаний и возможностей их эффективного использования. К тому же, скорость устаревания знаний требует не только формирования мобильных систем переподготовки управленческих кадров, но и систематического самообразования. При этом особое внимание должно уделяться техническому и управленческому образованию, обеспечивающим способность специалистов к разработке нестандартных решений.

В связи с изменением задач, которые предстоит решать будущим менеджерам появятся такие новые профессии в области менеджмента, как тайм-брокер, экоаудитор, трендовый форсайтер, модератор сообществ пользователей, менеджер по кросс-культурной коммуникации, персональный бренд-менеджер, координатор программ развития сообществ и др.

Помимо профессиональных компетенций современный менеджер должен обладать социальными и личностными компетенциями. На самом деле для достижения настоящего успеха в бизнесе необходимы глубокие внутренние осознания, неразрывно связанные с духовной стороной жизни. Эти составляющие не противоречат, а скорее дополняют друг друга [10].

Управленческий персонал в условиях изменяющихся концепций, стратегии, бизнес-модели развития компании должен также обладать

знаниями и навыками преобразования организационной структуры и построения эффективной системы мотивации и стимулирования сотрудников. Прогнозируется, что в цифровой экономике промышленные компании будут все дальше уходить от иерархической архитектуры к моделям, базирующимся на сетевом взаимодействии и сотрудничестве. Они будут функционировать на основе распределенных команд, удаленных сотрудников и динамичных по составу коллективов с непрерывным обменом данными и знаниями о вещах или задачах, над которыми ведется работа [11].

Еще большие возможности с точки зрения реализации знаний и профессиональных навыков в перспективе будет представлять людям экономика по требованию: она будет вносить запросы компании, связанные с необходимостью выполнения конкретных видов работ или проектов в виртуальное облако. В нем будет осуществляться подбор специалистов и менеджеров, обладающих необходимыми компетенциями, находящихся в любой стране мира. В свою очередь для людей, пребывающих в виртуальном облаке, будут обеспечены такие личностные ценности, как свобода, отсутствие стрессов, высокий уровень удовлетворенности работой [49].

Многим отечественным и даже зарубежным компаниям такие перспективы не кажутся ближайшей реальностью. На последнем Всемирном экономическом форуме в Давосе отмечалось, что только 29% опрошенных промышленных компаний начали внедрять в производство интернет-вещей, 41% компаний все еще проводят пилотные испытания, а 30% даже не начинали тестировать технологии [45]. Важнейшими причинами сложившейся ситуации являются недостаточное осознание предпринимателями значимости и эффективности новых технологий и консервативное мышление руководителей компаний и финансовых институтов.

Представляется необходимым выделить следующие важные компетенции для сотрудников, занятых в цифровую эпоху. Первой важной компетенцией является способность обрабатывать БМД и вычленять из неё наиболее существенные фрагменты, несущие смысловую нагрузку. Значимость указанной компетенции проявляется в контексте нарастания количества окружающих нас данных. Такая компетенция позволяет нам определять наиболее перспективные направления развития, алгоритмы действий и принятия экономических решений.

Необходимо отметить, что вычленение информации происходит на основании внутренних ценностей каждого сотрудника. Именно внутренние представления позволяют нам развивать различные сферы деятельности. Следовательно, второй важной компетенцией является

способность расставлять приоритеты в собственном развитии и понимать структуру собственных знаний и навыков.

Умение создавать новые рынки также является важной компетенцией в условиях цифровизации экономики. Сегодня выделяется такое понятие как «интеллектуальное лидерство». Эта компетенция определяет способность к предвидению развития ситуации и обозначения наиболее перспективных предвосхищающих действий [36].

В настоящее время развитие технологий происходит стремительно, ежедневно появляются всё новые и новые мобильные приложения, обеспечивающие удовлетворение человеческих потребностей [57]. В этой связи, навык предвидения и формирования новых рынков является важной компетенцией в условиях цифровизации экономики. Данный навык занимает одно из лидирующих положений в контексте стратегического развития.

Стоить отметить, что происходит смещение от компетенций, обеспечивающих комфорт и стабильность развития к компетенциям, обеспечивающим динамическое развитие и инновационный рост. Другим важным вопросом наряду с перечнем компетенций, диктуемых развивающимся информационным обществом, является возможность их формирования посредством использования существующих в настоящее время общественных институтов. Анализ российской специфики указывает на наличие существенных деформаций в механизмах взаимодействия власти, бизнеса, системы образования и самих наемных работников [18].

В России создана система формирования компетенций, в рамках которой регулирующие функции государства возложены на Министерство образования и науки РФ. Существующая система регулирования ограничена жесткими требованиями образовательных стандартов, что существенно сужает возможности российских ВУЗов по реализации образовательных программ с использованием современных гибких форматов обучения, ориентированных на запросы реального бизнеса. В отличие от российских, зарубежными образовательными организациями часто предоставляется открытый доступ к образовательным программам и курсам. Данный механизм подразумевает самостоятельное изучение курса с последующей сдачей сертификационного теста. В российских ВУЗах делаются попытки по внедрению данных механизмов, но необходимо признать, что в настоящий момент данная система находится в зачаточном состоянии. Указанные факторы способствуют консервации существующей системы предоставления образовательных услуг, не формирующих у специалистов набор компетенций, востребованных в эпоху цифровой экономики. Вместе с тем со

стороны государства прилагаются существенные усилия, направленные на ужесточение регулирования деятельности коммерческих вузов. Это объясняется репутационными рисками, связанными отсутствием у многих таких ВУЗов необходимого аудиторного фонда и преподавательского состава, обеспечивающего качество предоставляемых образовательных услуг. Также негативным фактором является низкий уровень контроля со стороны таких ВУЗов за процессом аттестации студентов.

Высокий уровень бюрократизации в государственных ВУЗах зачастую отпугивает представителей реального сектора экономики от сотрудничества. Некоторая часть наиболее крупных компаний идет по пути создания собственных кафедр на базе опорных ВУЗов для подготовки сотрудников под нужды конкретной компании. Ряд компаний идут по другому пути, создавая и развивая собственные корпоративные университеты. В условиях цифровой экономики наметилось увеличение доли на рынке небольших инновационных предприятий, у которых отсутствуют необходимые средства для создания таких структур. Фактически такие компании зачастую бывают лишены человеческих ресурсов, обладающих необходимыми компетенциями.

Одним из возможных направлений по созданию системы ориентированный на подготовку специалистов, обладающих компетенциями, востребованными в рамках цифровой экономики, является формирование электронных курсов на базе университетов под нужды конкретных компаний и дальнейшая подготовка сотрудников на базе корпоративных университетов или учебных центров компаний. Фактически такая технология подразумевает слияние двух имеющихся в настоящее время систем воедино [21].

Подготовка кадров для современной экономики и промышленности в условиях «цифровой экономики» и «Индустрии 4:0» – это вызовы для российского высшего образования конца второго десятилетия XXI века [19].

Современные студенты практически все используют инструменты ИКТ для личного, внутригруппового и межгруппового общения: создают свои сообщества в социальных сетях, активно используют мессенджеры и технологии мгновенных коммуникаций в режиме реального времени (WatsApp, Telegram и др.).

Задача развития цифровой экономики тесно связана с развитием отраслей, входящих в так называемую «экономику знаний» – образование, здравоохранение, IT-технологии, биотехнологии, – являющиеся решающим фактором повышения качества жизни человека. Они

окажут воздействие на развитие человеческого капитала: развитие интеллекта, знаний, здоровья.

Сегодня международные эксперты относят Россию к группе ведущих стран с точки зрения развития цифровой экономики. Однако по сравнению со странами-лидерами в этой области мы отстаем на пять-восемь лет. И медлить нельзя, так как существует серьезная опасность отстать навсегда. Поэтому сегодня наша страна должна сделать все, чтобы остаться ведущей технологической державой, не потерять свои преимущества во время новой научно-технической революции.

Резюмируя вышесказанное, можно сделать вывод, что развитие системы формирования компетенций сотрудников в эпоху цифровой экономики по обозначенному нами сценарию позволит существенно повысить ее эффективность.

# ГЛАВА 2. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЦИФРОВОГО ПРОСТРАНСТВА КАК ПРИОРИТЕТНОЕ НАПРАВЛЕНИЕ РАЗВИТИЯ ЦИФРОВОЙ ЭКОНОМИКИ

## 2.1. Информационная безопасность в системе национальной безопасности

Под информационной безопасностью (ИБ) понимают состояние защищенности информации и информационной среды от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, (в том числе владельцам и пользователям информации) [86].

Защита информации – комплекс мероприятий, направленных на обеспечение информационной безопасности.

Существует также одноименная учебная (научная) дисциплина — сравнительно молодая, но динамично развивающаяся отрасль ИТ, занимающаяся изучением (разработкой) средств, методов и моделей защиты информации.

Самая распространенная модель ИБ базируется на обеспечении трех свойств информации: конфиденциальность, целостность и доступность.

Конфиденциальность информации означает, что с ней может ознакомиться только строго ограниченный круг лиц, определенный ее владельцем. Если доступ к информации получает неуполномоченное лицо, происходит утрата конфиденциальности.

Для некоторых типов информации конфиденциальность является одним из наиболее важных атрибутов (например, данные стратегических исследований, медицинские и страховые записи, спецификации новых изделий и т. п.). В определенных случаях важно сохранить конфиденциальность сведений о конкретных лицах (например, сведения о клиентах банка, о кредиторах, налоговые данные; сведения медицинских учреждений о состоянии здоровья пациентов и т. д.).

Целостность информации определяется ее способностью сохраняться в неискаженном виде. Неправомочные, и не предусмотренные владельцем изменения информации (в результате ошибки оператора или преднамеренного действия неуполномоченного лица) приводят к потере целостности. Целостность особенно важна для данных, связанных с функционированием объектов критических инфраструктур (например, управления воздушным движением, энергоснабжения и т. д.), финансовых данных.

Достаточно показателен пример, когда злоумышленник вторгся в компьютерную систему исследовательской лаборатории ядерной физики в Швейцарии и изменил один знак в значении числа «пи», в результате чего из-за ошибок в расчетах был сорван важный эксперимент, а организация понесла миллионные убытки.

Доступность информации определяется способностью системы предоставлять своевременный беспрепятственный доступ к информации субъектам, обладающим соответствующими полномочиями. Уничтожение или блокирование информации (в результате ошибки или преднамеренного действия) приводит к потере доступности.

В настоящее время происходит переход от индустриального к информационному обществу. Материальные и энергетические ресурсы становятся менее важными, чем информация. В постиндустриальном (информационном) обществе информация выходит на уровень самостоятельного фактора производства.

В век ИКТ и стремительного развития сферы информационных услуг классическая фраза Н. Ротшильда «Кто владеет информацией, тот владеет миром» отражает суть современного мира.

В современном мире изменяется структура самой экономики - все больше людей занимаются не производством товаров, а получением и обработкой информации [104]. На смену привычной для всех экономики приходит эпоха цифровой экономики, обладающей рядом особенностей:

- основным ресурсом становится информация, которая неиссякаема;
- торговые площади в Интернете не имеют ограничений;
- размеры компании не влияют на ее конкурентоспособность;
- один и тот же физический ресурс может быть использован бесконечное количество раз для предоставления различных услуг;
- масштаб операционной деятельности ограничивается только мощностью Интернета.

Понятие «информационное общество» стало применяться со второй половины 1960-х годов, ввёл данный термин в научный дискурс японский ученый Ю. Хаяши, профессор Токийского технологического института. Информационное общество определялось им как такое, где процесс компьютеризации даст людям доступ к надежным источникам информации, избавит их от рутинной работы, обеспечит высокий уровень автоматизации производства. При этом изменится и само производство – продукт его станет более «информационно емким», что

означает увеличение доли инноваций, дизайна и маркетинга в его стоимости.

Опираясь на количественные меры математической теории информации, Д. С. Робертсон (США), который, исходя из взаимообусловленности цивилизационного и информационного процессов, выдвинул формулу «цивилизация – это информация», по количеству производимой информации проранжировал уровни развития цивилизации следующим образом:

• уровень 0 – информационная емкость мозга отдельного человека – 107 бит;

• уровень 1 – устное общение внутри общины, деревни или племени – количество циркулирующей информации 109 бит;

• уровень 2 – письменная культура; мерой информированности общества служит Александрийская библиотека, имеющая 532800 свитков, в которых содержится 1011 бит информации;

• уровень 3 – книжная культура: имеются сотни библиотек, выпускаются десятки тысяч книг, газет, журналов, совокупная емкость которых оценивается в 1017 бит;

• уровень 4 – информационное общество с электронной обработкой информации объемом 1025 бит» [132].

Становится очевидным, что экономика информационного общества нацелена на поддержку возрастающего информационного обмена и гармонизацию возникающих диспропорций между ростом производства материальных благ (в соответствии с законом возрастания потребностей) и растущим отвлечением общественных ресурсов в информационную «непроизводственную» сферу.

С точки зрения экономической теории можно сказать, что информация способна оказывать влияние на рост производительности труда и создание прибавочной стоимости в материальной составляющей производства общественного богатства и это является ее первичным экономическим содержанием в экономике информационного общества [81]. Информация как «сырье» создается человеком, природой и различными техническими устройствами. Ими же она потребляется, а для переработки требует решения вопросов передачи, хранения, поиска и доведения, для чего создается «транспорт» (магистральные и локальные сети, системы связи), «склады» (дата-центры), «техника» (компьютеры), «инструменты» (программное обеспечение). То есть в экономике формируется определенный сегмент материального производства и сферы услуг для удовлетворения информационных потребностей общества.

Цифровая экономика или, другими словами, веб-экономика представляет собой систему экономических, социальных и культурных отношений, строящихся с использованием современных цифровых технологий.

В Указе «О стратегии развития информационного общества в Российской Федерации на 2017-2030 годы» отражены цели и стратегические национальные приоритеты при развитии информационного общества государства. В этом документе цифровая экономика определяется как «…- хозяйственная деятельность, в которой ключевым фактором производства являются данные в цифровом виде, обработка больших объемов и использование результатов анализа которых по сравнению с традиционными формами хозяйствования позволяют существенно повысить эффективность различных видов производства, технологий, оборудования, хранения, продажи, доставки товаров и услуг», а под экосистемой цифровой экономики понимается «…– партнерство организаций, обеспечивающее постоянное взаимодействие принадлежащих им технологических платформ, прикладных интернет-сервисов, аналитических систем, информационных систем органов государственной власти Российской Федерации, организаций и граждан» [1].

Кроме этого, на основную стратегию развития информационной составляющей экономики влияет принятая в России «Программа развития цифровой экономики в Российской Федерации до 2035 года». В программе определены основные цели [93].

Установлены направления развития цифровой экономики: нормативное регулирование, кадры и образование, формирование исследовательских компетенций и технических заделов, информационная инфраструктура и информационная безопасность. Основополагающие принципы информационной безопасности включают использование российских технологий, отечественного программного обеспечения и оборудования, российских криптографических стандартов. Предусмотрено формирование системы управления цифровой экономикой. Одна из важнейших ее задач - поддержка «стартапов» и субъектов малого и среднего бизнеса в области разработки и внедрения цифровых технологий. Установлены показатели программы, которых необходимо достичь к 2024 г.» [93]. Основная цель всех этих нормативно-правовых актов – это повышение качества жизни граждан России и обеспечение конкурентоспособности государства и национальной безопасности.

Цифровая экономика становится повседневной реальностью современного общества, благодаря ее использованию повышается эффективность всех отраслей. Качественно и количественно увеличиваются возможности использования современных компьютерных технологий - через компьютер можно совершать практически все операции: оплачивать услуги, заказывать билеты, очереди, искать необходимую информацию и т.д. Информация в эру цифровой экономики играет важнейшую роль, она становится основным нематериальным активом, имеющим огромную ценность [102].

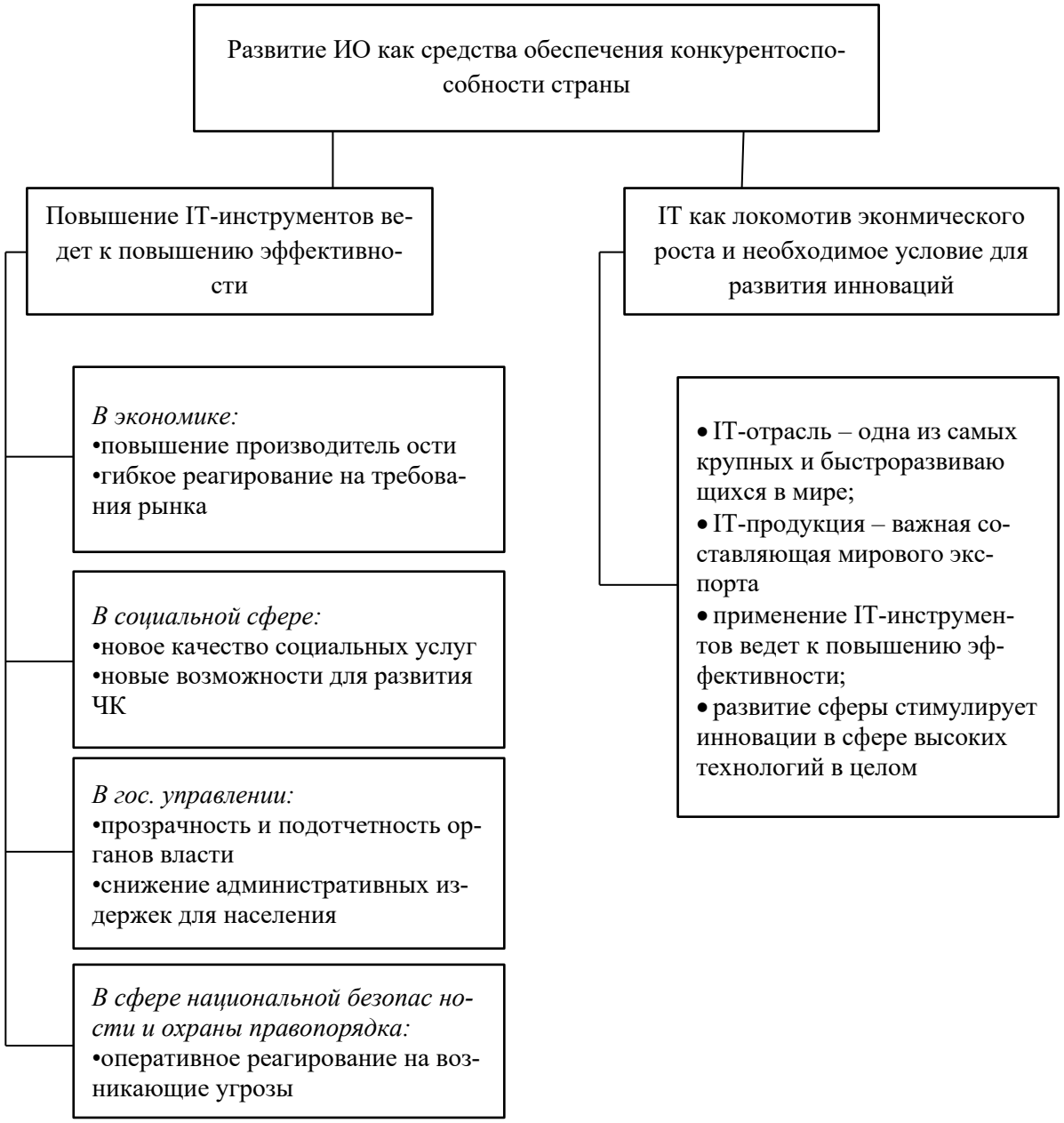



**Рисунок 9** – Ключевые факторы развития информационного общества

Главная тенденция в развитии информации на современном этапе состоит в совершенствовании компьютерной техники в сочетании с достижениями в области искусственного интеллекта и средств коммуникации. На рисунке 9 схематично представлены ключевые моменты повышения конкурентоспособности государства при условии развития информационного общества.

В современном мире информация становится основой социальных ценностей общества. ИТ стали важнейшей составляющей процесса использования обществом информационных ресурсов. К настоящему времени они завершили несколько эволюционных этапов, смена которых обуславливалась, главным образом, прогрессом технологий, появлением более современных технологических средств для поиска и обработки информации. Современный этап развития характеризуется изменением направленности сегмента ИТ с развития технической базы на применение доступных средств для создания стратегического преимущества [115].

В 2017 году цифровая революция вошла в решающую фазу – к интернету подключился каждый второй житель Земли. По оценке Глобального института McKinsey (MGI), уже в ближайшие 20 лет до 50% рабочих операций в мире могут быть автоматизированы, и по масштабам этот процесс будет сопоставим с промышленной революцией XVIII–XIX веков [123].

Общественная информатизация является реакцией на многократный рост информационных мощностей, темпов потребления информационных ресурсов и необходимости в значительном увеличении производительности труда в информационном секторе общественного производства. Как показывает практика стран с развитой экономикой, таких как США, Японии и стран Евросоюза, решение проблемы информатизации общества является глобальной целью развития и связывается с выходом планеты на новый уровень цивилизации.

Одним из признаков цифровой экономики является высокая скорость. Возрастание скорости происходит везде, но в особенности это касается выполнения заказов, создания, получения или отправки информации. От любого действия ожидается мгновенная реакция [119].

Цифровая экономика стремительно вытесняет старый уклад во всех сферах деятельности современного общества, позволяет автоматически выполнять рутинные операции и быстро предоставлять информацию для принятия оптимальных решений. Ключевую роль в цифровой экономике занимают информационные системы. Для оператора связи такими системами в первую очередь являются системы

поддержки операций (OSS) и системы поддержки бизнеса (BSS). Так как они представляют собой категорию прикладного обеспечения внутренних бизнес-процессов, то их трансформация — это реакция на изменения в бизнес-процессах.

На рисунке 10 представлены свойства данных, информации и знаний.

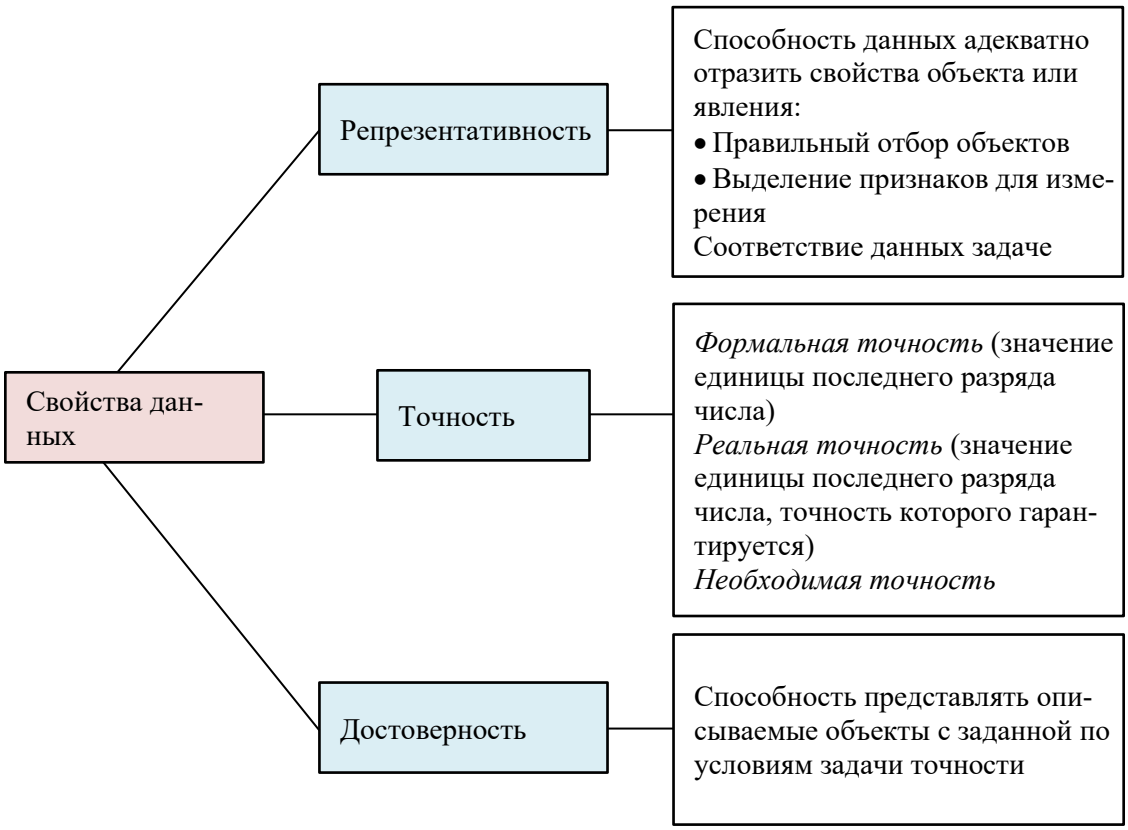



**Рисунок 10** – Свойства данных, информации и знаний

С применением ИТ происходит трансформация во всех слоях общества, в частной жизни, изменяется уклад жизни людей. Возникает потребность в новых профессиях и инструментах взаимодействия. Возрастает роль электронных ресурсов, представляющих собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом отношений [116].

Стремительный рост компьютерных технологий в различных сферах человеческой деятельности, с одной стороны, позволил обеспечить высокие достижения в этих сферах, а с другой стороны, стал источником самых непредсказуемых и вредных для человеческого

общества последствий. В результате, можно говорить о появлении принципиально нового сегмента международного противоборства, затрагивающего как вопросы безопасности отдельных государств, так и общую систему международной безопасности на всех уровнях [72, 73].

На рисунке 11 представлена взаимосвязь информатизации общества.

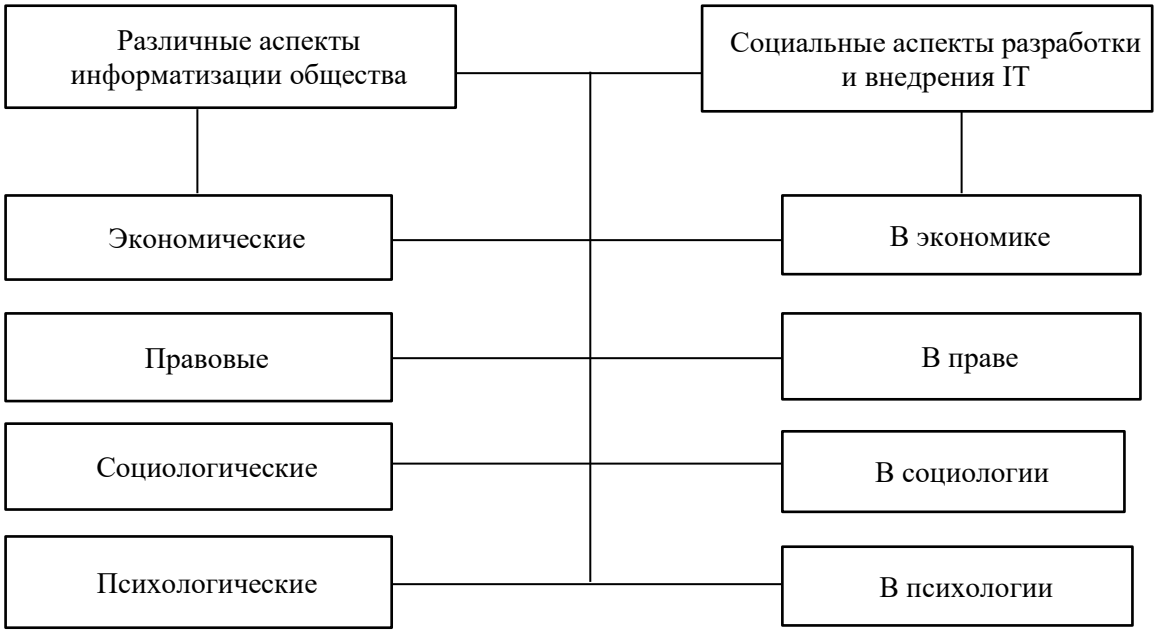



**Рисунок 11** – Категории, понятия, закономерности информатизации общества

Информационное пространство любой страны призвано выполнять определенные стратегические и тактические функции. Стратегические, направленные на создание новой социальной идентичности, защиты от вторжения чужой информации, реализуются посредством новостной и художественной коммуникации. Тактические, которые способствуют решению конкретных задач социального управления, организации поддержки властных инициатив, информирования населения о краткосрочных событиях, выполняются в основном новостными коммуникациями. И стратегические, и тактические функции служат для выработки единых моделей интерпретации действительности, особенно в кризисные периоды [118].

В различные периоды развития общества есть как свои плюсы, так и минусы. Соответственно различным аспектам информатизации общества, к плюсам развития цифровой экономики Всемирный банк в своем обзоре 2016 года «Цифровые дивиденды» относит:

– рост производительности труда;

– повышение конкурентоспособности компаний;

– снижение издержек производства;

– создание новых рабочих мест [13];

– преодоление бедности и социального неравенства [92].

И это всего лишь несколько примеров того, как цифровая экономика положительно влияет на нашу жизнь, давая множество возможностей рядовому пользователю, и тем самым расширяя возможности самого рынка.

Однако, наряду с большим количеством преимуществ, цифровая трансформация несет и определенные риски:

– риск киберугроз;

– использование данных о людях для управления их поведением;

– рост безработицы, исчезновение определенных профессий [32];

– разрыв в цифровом образовании и как следствие разрыв в благосостоянии;

– и т.д.

Жизненно важные интересы субъектов (государства, юридических и физических лиц), участвующих в процессах автоматизированного взаимодействия, как правило, заключаются в том, чтобы определенная часть информации, касающаяся их экономических, политических и других сторон деятельности, конфиденциальные коммерческие и персональная данные были бы легко доступны и в то же время надежно защищены от неправомерного использования [127]. Искажение или фальсификация, уничтожение или разглашение определенной части информации, равно как и дезорганизация процессов её обработки и передачи, наносят серьезный материальный и моральный урон.

На рисунке 12 приведены основные «плюсы» и «минусы» информационного общества.

Компании, являющиеся пионерами цифровой революции, не только получают значительные преимущества, но и несут повышенные риски. Одним из острейших вопросов современности является вопрос обеспечения информационной безопасности, как различных госструктур, так и коммерческих организаций и персональных данных. «В последнее время, все большие объемы информации, в том числе и критически важной для отдельных людей, организаций или государств, хранятся, обрабатываются и передаются с использованием АС обработки информации. Система обработки информации – совокупность технических средств и программного обеспечения, а также методов обработки информации и действий персонала, необходимых для выполнения автоматизированной обработки информации» [66].


**Рисунок 12** – Основные плюсы и минусы информационного общества

Даже полтора десятилетия назад, когда информационная экономика была на начальных стадиях внедрения в нашу жизнь, согласно исследованиям специалистов по информационной безопасности – уже к тому времени все больше был заметен перекос понятий в области защиты данных. Говоря об экономической целесообразности мер по поддержке информационной безопасности, многие в первую очередь имеют в виду защиту от вирусов и хакеров, но наибольший вред, согласно отчётам ведущих организации последние десять лет приносят действия инсайдеров (сотрудников компании), что показано, к примеру, в ежегодных отчетах ФБР Computer Crime and Security Survey.

Таким образом, согласно данным этих исследований, оцениваемый ущерб от неосторожных и неправомерных действий сотрудников в разы превышает объем причиненного вреда от действий вирусов и хакерских атак, или же попыток вредоносного непосредственного внедрения с целью извлечения информации. И это было ещё в 2007 г.,

когда количество инцидентов по вине внешних и внутренних нарушителей спокойствия было соизмеримо.

Этот результат был вполне закономерен. Несмотря на то, что внешних злоумышленников действительно значительно больше, но, во-первых, они меньше мотивированны, отбросив малое число наемных профессионалов, мы получим огромную массу школьников и студентов, которые просто из любопытства пробуют скачанные утилиты, не преследуя каких-либо определенных целей и порой даже не зная, что делать с полученной информацией. Во-вторых, им противостоят мощные и зрелые технологии периметровой защиты, то есть внешнему злоумышленнику нужна большая квалификация, чтобы преодолеть все эти барьеры.

В наше время, даже несмотря на значительное улучшение технологий прорыва через средства сетевой и информационной безопасности – ситуация не особо изменилась. Чаще всего от внешних ударов страдают именно стратегически важные направления или крупнейшие предприятия, которым действительно можно либо нанести непоправимый ущерб с помощью нарушения их информационной безопасности, кражи данных или средств, в случае финансовой организации. Что же касательно малого и среднего бизнеса, то он всё так же редко попадает под удар, поскольку не представляет особого интереса, даже учитывая значительно более слабые средства защиты от вмешательства извне.

У внутреннего же нарушителя, особенно в том случае, если его действия сознательны, а не являются ошибкой, стимулов может быть больше. От банальной обиды до материальной выгоды в случае подкупа со стороны конкурентов, а возможностей при этом значительно больше, поскольку он изначально уже является легальным пользователем сети, имеет доступ, в том числе, и к конфиденциальным ресурсам организации, может пользоваться корпоративными приложениями и обрабатываемыми в них данными на законных основаниях. Кроме того, примерно в 40% случаев внешнего вмешательства в работу предприятия – обхода системы информационной безопасности не происходит, банально из-за того, что для удара использовались внутренние ресурсы предприятия и заинтересованные штатные его сотрудники. Но если это так, почему большие усилия тратятся именно на защиту от внешних угроз? На это есть несколько причин.

Для начала, строить систему защиты от внешнего врага почти всегда является гораздо более простой задачей. Это хорошо известный и уже проторенный путь, так как любой из сотрудников информационной безопасности даже с низким уровнем квалификации готов начать

перечислять необходимые средства защиты от угроз, ибо они в большинстве случае схожи, а детали требуют адаптивности к определённой ситуации уже на месте, когда происходит попытка вмешательства. Кроме того, занимаясь построением внешнего рубежа обороны, от внешних же угроз – никто не влияет на работоспособность самой информационной системы. Все бизнес-приложения работают нормально, цена ошибки администрирования – по большому счету, лишь кратковременное отсутствие доступа в Интернет или небольшие нарушения в работе внутренней сети ресурсов, относящиеся к быстроустранимым проблемам.

Защита же от внутреннего врага на порядок сложнее и требует больших усилий, равно как и затрат. Она складывается из обеспечения безопасности самих приложений и грамотного администрирования, которое, прежде всего, подразумевает под собой наличие четких привилегий сотрудников компании на доступ к ресурсам информационной системы, которые в сформулированном виде называются внутренней политикой безопасности. Данные привилегии должны быть достаточны для обеспечения нормальной работы и в то же время минимальны с точки зрения доступа и возможности манипулирования информацией. Подобные системы контроля внутреннего доступа к настоящему времени используются многими предоставляющими услуги информационной безопасности лицами, будучи скопированными с государственной системы уровней допуска к секретной информации, только спроецированные уже на внутреннюю структуру компании. И зачастую при появлении подобной задачи, проблем видится больше, чем решений.

Перечислять их можно долго, так как основные проблемы цепляются друг за друга. Например, незащищенность ряда приложений вынуждает нас использовать дополнительные средства защиты, однако эти средства нужно не только приобрести и правильно внедрить, но и сопровождать на постоянной основе для каждого индивидуального устройства, используемого в компьютерной сети. И если с процессом внедрения обычно проблем не возникает, поскольку с оным справляются либо штатные специалисты, либо нанятые консалтинговые компании, трудности сопровождения появляются потом, в процессе администрирования системы. Ведь управление сопровождаемыми средствами защиты осуществляется зачастую отдельно от уже используемых в компании, в том числе и штатных механизмов. А это означает, что рано или поздно, в зависимости от масштаба информационной системы, наступает момент, когда настройки системы защиты и

настройки штатных механизмов начинают в значительной мере расходиться.

Расхождение происходит еще и потому, что отсутствуют процедуры, регламентирующие внесение изменений, как в саму информационную систему, так и в настройки подконтрольных ей механизмов безопасности. А, собственно, само внесение изменений в реальные настройки системы гораздо проще и быстрее, чем регулярное оформление оных с документированием основных внесённых поправок. Да и набрать номер администратора или забежать к нему по пути проще, чем написать заявку. В результате – в определённый момент времени практически невозможно воссоздать реальную картину происходящего, равно как и невозможно ответить на вопрос – почему к определенному ресурсу имеют доступ эти пользователи или группы пользователей, которые не обладают для подобного достаточными привилегиями. Именно подобным образом и теряется история всех производимых обновлений, а следственно уже нельзя определить - правильно ли или неправильно сконфигурированы, пусть даже самые совершенные, механизмы защиты.

Цена ошибки за подобное неправильное администрирование измеряется либо предоставлением пользователю необоснованно больших компетенций, то есть, при определённых прецедентах, это будет чревато созданием огромной уязвимости в информационной системе, либо ограничением необходимого ему в какой-то момент доступа, допустимого для его уровня привилегий, при этом, возможно, срывается выполнение задач самой организации.

Формально, существуют несколько способов решения указанных проблем, такие как внедрение полноценной системы централизованного управления и внедрение системы учета настроек и изменений в настройках информационной системы или любого из сегментов IT-сферы предприятия, даже вне юрисдикции отдела по информационной безопасности. Однако же, универсальная консоль управления всеми приложениями не спасает, поскольку подобное решение не дает ответ на вопрос – на каком основании, кто и как должен принимать решения о том, какие изменения нужны. Для упорядочения деятельности по администрированию на предприятии должны вырабатываться полноценные регламенты и прочие документы, описывающие правила работы и взаимодействия всех субъектов информационной системы.

Но при этом стоит помнить, что решить эту проблему только организационными методами не удается. Виной всему такие вещи как банальная нехватка и недостаточная квалификация администраторов,

перегруженность специалистов и, самое главное – отсутствие механизмов проверки фактического положения дел. Все это приводит к тому, что даже при наличии некоторой формальной системы управления контроль над информационной системой и вопросами безопасности данных в ней все равно теряется без адекватных мер управления. Поэтому, учитывая подобные процессы, стоит отметить, что часто простое увеличение штата IT-подразделения и подразделения информационной безопасности, даже только за счёт специалистов по администрированию – зачастую могут усугубить проблемы. В этих структурах, в свою очередь, появляются подразделения, специализирующиеся на отдельных подсистемах, взаимодействие структур нарушается еще больше, и поэтому, осознавая всю сложность решения задачи, а также отсутствие инструментов, специалисты по информационной безопасности зачастую медлят с устранением проблемы.

Обеспечение повышенных требований к информационной безопасности предполагает соответствующие мероприятия на всех этапах жизненного цикла ИТ. Планирование этих мероприятий производится по завершении этапа анализа рисков и выбора контрмер. Обязательной составной частью этих планов является периодическая проверка соответствия существующего режима политике безопасности, сертификация информационной системы (технологии) на соответствие требованиям определенного стандарта безопасности. Все перечисленное и есть управление рисками [67].

По большому счету, для управления любой сложной системой необходимо создать жесткий, но простой регламент обслуживания системы и обеспечить контроль за тем, чтобы настройки системы изменялись в соответствии с этим регламентом. Применительно к обеспечению безопасности информационной системы это можно представить следующим образом. Вначале включить в наличие документ, в котором должно быть четко описано, кто и на каком основании должен иметь доступ к ресурсам информационной системы. Кроме того, необходимо иметь единую точку взаимодействия сотрудников организации с информационной системой, через которую они смогут формулировать свои пожелания на предоставление доступа к тем или иным ресурсам информационной системы в рамках текущих норм информационной безопасности предприятия. И для управления подобными процессами предприятию необходимо иметь гибкие инструменты контроля правильности настроек информационной сети. Стоит отметить, что последние годы разработками такого рода уже занимается несколько крупных корпораций. Свои решения предлагают подразделения

информационной безопасности компаний Oracle и IBM. Отрадно, что в ряду гигантов IT-индустрии есть и отечественный разработчик, компания ПАО «Информзащита», которая имеет свою систему комплексного управления безопасностью, используемую внутри страны на государственных предприятиях. Особенность предлагаемых решений подобного рода состоит в том, что в них соединяются не работающие по отдельности технический и организационный подходы к управлению безопасностью.

При внедрении таких систем предполагается, что организация уже имеет сформулированную политику безопасности. Эта политика вместе с информацией об ИС служит в дальнейшем фундаментом системы управления. Что же касательно самого описания информационной системы обычно необходимо знать следующее:

1) Перечень информационных ресурсов. Под ресурсом могут пониматься конкретные серверы и папки на них, эксплуатируемые приложения, оборудование и даже сегменты сети.

2) Ответственный за безопасность этих ресурсов. Это могут быть владельцы ресурсов, главы подразделений, кураторы со стороны службы безопасности и другие.

3) Ответственный за администрирование этих ресурсов.

4) Как ресурсы информационной системы взаимосвязаны между собой. Порой для нормальной работы приложения необходим комплекс настроек – от настроек самого приложения до коммутационного оборудования. Ведь даже если мы выполним все настройки, но забудем прописать разрешающее правило на внутреннем межсетевом экране, решение всей задачи будет сорвано.

5) Штатная структура компании. Какой доступ и к каким ресурсам имеет сотрудник, занимающий определенную должность.

Таким образом, на базе всей вышеуказанной, полученной информации система управления выстраивает идеальную модель информационной сети предприятия, соответствующей нормам информационной безопасности. Этот момент можно считать стартовым в работе системы управления безопасностью. Отныне всё общение по вопросам изменений настроек информационной системы начинает происходить через специализированную систему документооборота, входящую в состав системы управления безопасностью, находящуюся под надзором отдела информационной безопасности.

Стоит отметить, что от зарубежных аналогов отечественную систему комплексного управления безопасностью отличает специальный транслятор, который позволяет преодолевать языковой барьер и

предоставляет возможность каждому работать с понятными ему терминами. К примеру, если это менеджмент компании – то в системе он может использовать набор функций по управлению сотрудниками и должностями, без лишних информационных надстроек, в то время как информационная безопасность и IT-специалисты будут работать учетными записями пользователей, их правами доступа и т. п.

Заявка на изменение доступа, составленная в системе управления безопасностью, будет проверена на непротиворечивость требованиям политики безопасности, согласована с владельцами ресурсов и направлена на выполнение администраторам. Выявлять несоответствие модели информационной системы и ее текущего состояния системе управления безопасностью позволяют агенты-сенсоры. Такие агенты регулярно следят за всеми связанными с сетевой безопасностью предприятия настройками операционных систем, приложений, средств защиты, сетевого оборудования.

Под несоответствием системы управления безопасностью информационной системы предприятия следует понимать либо невыполненные администратором необходимых действий по администрированию информационной системы, либо действия, совершенные им в обход принятого и утвержденного в организации порядка. Например, предоставление лишних полномочий какому-либо пользователю или неправомерное ограничение пользователя в правах.

Информация о несоответствиях тут же поступает в службы безопасности и в службу IT. Ведь каждое из них связано с тем, что кто-то из сотрудников либо приобретает права на доступ к ресурсам информационной системы, либо теряет их. Это означает, что он может получить лишнюю информацию или лишиться доступа к необходимым ему сведениям. А это, как уже отмечалось, равнозначно недопустимо, поскольку таит угрозу безопасности или же приводит к срыву выполнения бизнес-задач.

Наличие в системе документооборота механизма архивирования заявок на изменения доступа к информационной системе позволит в любой момент понять, кто имеет доступ к ресурсам информационной системы, и кто запрашивал предоставление этого доступа. Использование описанного подхода к управлению информационной безопасностью — это серьезные изменения в привычном ритме работы информационной системы. Но затраченные усилия с лихвой окупятся. Выгоды от внедрения систем управления безопасностью очевидны. И прежде всего это повышение защищенности информационной системы, поскольку отныне все производимые изменения настроек будут

контролироваться и производиться в точном соответствии с политикой информационной безопасности организации. Дополнительным бонусом будет сокращение издержек на сопутствующий управлению документооборот.

Кроме того, после внедрения подобной системы управления обеспечение информационной безопасности перестает быть уделом, ответственностью и обязанностью только узких специалистов. В управлении информационной системой начинает действительно активно принимать участие менеджмент организации: ведь именно они теперь формируют требования к настройкам посредством механизма заявок.

Что же касательно самого рынка информационной безопасности в нашей стране, то тут ситуация выглядит следующим образом. В России к вопросам информационной защиты наиболее серьезно подходят компании, имеющие отношение к ИТ, к банковскому сектору, сотовой связи, компании, проводящие операции с ценными бумагами. Что касается других организаций, согласно результатам различных исследований, руководители многих из них знают об основных видах угроз, но не уделяют должного внимания этим вопросам, полагая, что обеспечение информационной безопасности не имеет смысла, если отсутствует видимая угроза. То есть основная проблема в сфере информационной защиты – недостаточное внимание к ней руководства компаний и, как следствие, дефицит ее финансирования.

Тем не менее, постепенно руководители российских компаний изменяют свой взгляд на информационную безопасность, начиная относиться к ней как к одному из способов повышения конкурентоспособности компании.

Переходя к структуре применяемых систем обеспечения комплексной информационной безопасности, стоит сказать, что, несмотря на значительный прогресс – в настоящее время львиную долю отечественного рынка информационной безопасности до сих пор составляют межсетевые экраны, системы обнаружения атак (Intrusion Detection Systems – IDS) и антивирусные системы. Однако эти средства в большинстве своём перестали удовлетворять современным требованиям, в рамках нынешних реалий информационной безопасности, предъявляемых к защитным системам.

Это вполне объяснимо, так как интервалы времени между появлением сообщения об очередной новой точке уязвимости в программном обеспечении, выпуском «заплатки» и созданием программы, использующей эту уязвимость, сокращаются сегодня очень быстро. IDS

всего лишь обнаруживают компьютерные атаки. Можно провести параллель между такой системой и термометром: последний лишь определяет температуру тела больного, но не является средством лечения. Получается, что система обнаружения компьютерных атак имеет только диагностическое значение.

Существуют две технологии обнаружения атак, первая из них это технология сигнатурного анализа, а вторая это так называемая технология выявления аномальной деятельности. IDS, основанные на первой из них, обнаруживают далеко не все атаки, а лишь те, которые уже описаны в сигнатурах (образец IP-пакета данных, характерного для какой-либо определенной атаки). Иными словами, они реагируют только на известные атаки и беззащитны перед новыми, неизвестными. Такие IDS работают по тому же принципу, что и антивирусные программы: известные вирусы ловятся, неизвестные – нет.

Появление новой сигнатуры всегда обусловлено анализом механизма уже прошедшей атаки и ее воздействия на какую-либо информационную систему. Хорошо, если это были действия, направленные на конкретные информационные ресурсы. А если это была, допустим, новая разновидность интернет-червя? Тогда пользователь защитной системы, созданной на основе технологии сигнатурного анализа, не застрахован от последствий возможной компьютерной атаки. Принцип работы «пронесет-не пронесет» устроит лишь тех пользователей, для которых не критична потеря информации, но не тех, чья деятельность основана на использовании информационных ресурсов.

Возникает резонный вопрос, а как же быть с неизвестными атаками? Случавшиеся в последнее время компьютерные атаки, например такие как Slammer или Nimda, ускользают от внимания программных средств, основанных на распознавании сигнатур, и практически мгновенно распространяются через локальные сети – задолго до того, как становится возможным какое-либо обновление систем защиты. Система, ориентированная на выявление новых типов атак, – это система выявления «аномального» поведения, которая отслеживает в сетевом трафике, в работе приложений и в других процессах все отклонения от нормы, контролирует частоту событий и обнаруживает статистические аномалии. Основанная на анализе поведения, такая система может остановить как известные, так и не встречавшиеся ранее виды несанкционированной деятельности. Однако и у нее есть существенный недостаток – трудности с формулировкой эффективных критериев того, что считать аномальным поведением, а что не считать. Объединяя эти

две технологии и устраняя таким образом их взаимные недостатки, можно получить средство обнаружения известных и неизвестных атак.

Необходимо не только обнаружение, но и блокирование вредоносных воздействий – переход к проактивной защите. Обнаружение вторжений без противодействия нельзя считать эффективным средством защиты. Приобретая систему информационной безопасности, пользователь преследует цель гарантированно защитить свои информационные ресурсы от злонамеренных действий. Поэтому на очередном витке развития ИТ, сталкиваясь с постоянной эволюцией угроз и следуя пожеланиям пользователей, разработчики средств информационной защиты предложили на смену IDS системы предотвращения компьютерных атак.

Основа функционирования IPS – интеграция IDS с межсетевыми экранами. Кроме того, обязательным условием эффективной работы IPS является установка системы «в разрыв» сети. Система IPS не только определяет, но и пытается остановить атаку, и даже может провести ответное нападение на атакующего. Наиболее распространенные типы реагирования – прерывание сессии и переконфигурирование межсетевого экрана. Сегодня IPS – уже превалирующая технология, реализованная в продуктах практически всех известных производителей средств информационной защиты. Некоторые вендоры идут дальше и пытаются дополнить системы предотвращения атак уникальными разработками.

Интересна в этом плане популярная технология Virtual Patch, разработанная специалистами компании Internet Security System, работающей в сфере информационной безопасности. Её главное предназначение – это блокирование атаки, эксплуатирующей уязвимость в определенной системе, до официального выпуска «заплатки» производителем этой системы. Фактическая скорость выхода обновления для модуля Virtual Patch составляет несколько часов с момента обнаружения первой информации об уязвимости, после чего происходит рассылка обновлений и автоматическая реконфигурация сенсоров системы обнаружения атак, так как воздействие системы точечное и не связано с традиционными средствами информационной безопасности.

По состоянию на сегодня внутренние нарушители представляют едва ли не большую опасность, чем внешние, ведь злоумышленником может быть любой сотрудник компании, от обычного пользователя до руководителя высшего ранга. И решение задачи защиты информации от несанкционированного воздействия внутренних пользователей невозможно только организационными, или только техническими

методами защиты. Лишь комплексное применение этих методов способно принести результат. Комплексная система защиты информации должна быть: непрерывной, плановой, целенаправленной, конкретной, активной, надежной и др. Система защиты информации должна опираться на систему видов собственного обеспечения, способного реализовать ее функционирование не только в повседневных условиях, но и критических ситуациях.

В связи со всем этим взаимосвязанным комплексом переменных, которые необходимо учитывать в современном информационном обществе, становится очевидным факт взаимосвязи всех сфер общественного регулирования. За последнее десятилетие усилилась роль информатизации образования в развитии информационного общества и их тесная взаимосвязь.

С одной стороны становление информационного общества существенно влияет на процессы проникновения ИТ во все сферы образовательной деятельности, с другой стороны информатизация образования формируя информационную культуру членов общества, существенно способствует его информатизации.

## 2.2. Информационная безопасность цифрового пространства Интернета вещей

В настоящее время цифровое пространство (среда) становится движущей силой преобразований во всех сферах жизнедеятельности личности, общества и государства [74]. Радикальные изменения вызваны двумя основными факторами: быстрым прогрессом (ИКТ) и их интеграцией в социотехнические системы наряду с массовой доступностью. Несомненно, проблемы ИБ, являются производными относительно более общих проблем цифрового пространства. При этом, в решении тех и других присутствует в явном или неявном виде «человеческий фактор» как один из важнейших аспектов. Особенность заключается в том, что человек из оператора, т.е. средства, превратился в цель функционирования информационной системы, массовый пользователь практически беззащитен лично и невольно может стать вредоносным агентом. Поэтому содержание проблем ИБ должно формироваться в соответствии с содержанием проблем цифровизации [96].

Цифровое пространство как цифровая среда – среда логических объектов, используемая для описания (моделирования) других сред (в частности, электронной и социальной) на основе математических

законов» создает проблему цифрового неравенства и цифрового суверенитета, сущность которых состоит в доминировании в различных сферах жизнедеятельности. Тогда как развитие сетевых технологий обусловливает проявление скрытого управления групповым и массовым поведением, то создание сетей со сложными и взаимосвязанными проблемами, такими как защита критической инфраструктуры на национальном уровне влечет за собой образование киберпространства [63]. В новых условиях только технические аспекты явно недостаточны для комплексного понимания проблематики ИБ. Поэтому роль человека в кибер-безопасности является всеобъемлющей [46].

Понятие «Интернет вещей» (Internet of Things, IoT) появилось в 1999 году. Существует несколько определений, раскрывающих суть данного понятия.

По версии компании IDC «Интернет вещей — это сеть сетей с уникально идентифицируемыми конечными точками, которые общаются между собой в двух направлениях по протоколам Internet Protocol (IP) и обычно без человеческого вмешательства».

Специалисты компании Gartner дают следующее определение: «Интернет вещей — это сеть физических объектов, которые имеют встроенные технологии, позволяющие осуществлять взаимодействие с внешней средой, передавать сведения о своем состоянии и принимать данные из вне».

Существует еще более технологичное определение компании McKinsey − «Интернет вещей — это датчики и приводы (исполнительные устройства), встроенные в физические объекты и связанные через проводные или беспроводные сети с использованием протокола IP, который связывает Интернет».

Другими словами, «Интернет вещей — это необъятное скопление подключенных датчиков, камер, смартфонов, компьютеров и устройств, которые взаимодействуют с приложениями, веб-сайтами, социальными медиа и другими устройствами. Чтобы извлечь из этого максимальную пользу, необходимо обрабатывать и анализировать данные, которые генерируют все эти объекты, в реальном времени».

Можно вывести условную формулу, характеризующую Интернет вещей (IoT) [98] (Рисунок 13).

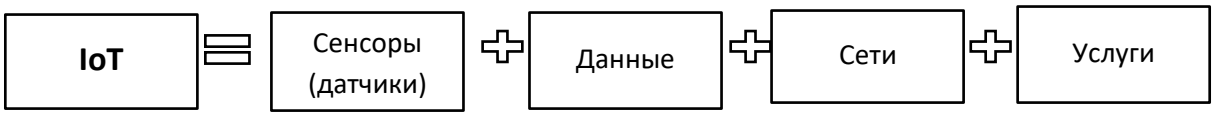



**Рисунок 13** – Образное представление интернета вещей

Решения для Интернета вещей базируются на использовании облачных технологий.

Под конкретной «Интернет вещью (thing)» принято понимать «любой натуральный или искусственный предмет, которому может быть присвоен IP-адрес и который обладает возможностью передачи данных по сети».

В 2009 году количество подключенных к сети предметов превысило количество людей, произошел переход от Интернета людей к Интернету вещей.

Ключевыми поставщиками для Интернета вещей, являются известные мировые компании: Alcatel-Lucent, Cisco, AT&T, Qualcomm, Amazon Web Services (AWS), Apple, ARM Holdings, Digi International, Atmel, Atos, Bosch Software Innovations, Broadcom, CTS, Dell, Echelon, Ericsson, Accenture, Freescale Google, Semiconductor, GE, Hitachi, HP, IBM, Huawei Technologies, Infosys и др.

Принято выделять решения Интернета вещей как для корпоративного сектора (B2B), так и для потребительского сектора (B2C). В потребительском секторе Интернета вещей преобладают бытовые (для дома) и носимые устройства (электроника), умная одежда, т.п. Корпоративный сектор решений для Интернета вещей представлен решениями для промышленного Интернета вещей (IIoT), умного города, электроэнергетики, здравоохранения, управления цепочками поставок, торговли, др.

В настоящее время решения Интернета вещей наиболее активно используются в технологиях «умного дома»: удаленное управление через Интернет домашними устройствами, удаленный мониторинг и управление системами отопления, освещения, медиа − устройствами, электронными системами безопасности, оповещениями о вторжениях, противопожарными системами и пр.

Интернет вещей плотно вошел в нашу жизнь и миллиардов людей по всему миру. Рост количества подключенных устройств ведет к увеличению рисков безопасности: от причинения физического вреда людям до простоев и повреждения оборудования [147].

Заинтересованными сторонами в создании защищенных решений являются участники рынка, владельцы систем и производители средств защиты. Спрос на «реальную защиту» сложных систем и решений только начал формироваться. Внедрение средств безопасности увеличивает совокупную стоимость владения для конечного пользователя. Компании не спешат финансировать создание систем защиты, т.к.

не видят экономической целесообразности, практической пользы и конкурентных преимуществ в краткосрочной перспективе.

Объем рынка в области безопасности Интернета вещей в 2019 г. прогнозируется по данным портала [5] на уровне 1,439 млн долларов. С ростом сегмента рынка решений для Интернета вещей эта цифра будет только увеличиваться.

Традиционно принято выделять следующие направления в области технологий безопасности Интернета вещей [5]:

− безопасность устройств (физическая безопасность, безопасность данных, встроенная безопасность на базе микросхем, безопасная загрузка, аутентификация устройств, управление идентификацией устройств);

− безопасность сетевого взаимодействия (механизмы доступа, файрволлы, системы обнаружения и защиты от вторжений, End-2-End шифрование);

− облачная безопасность (безопасность данных, системы предотвращения утечек, интеграция платформ и приложений, управление угрозами);

− управление безопасностью в процессе жизненного цикла (управление рисками, политиками, аудит безопасности, мониторинг эксплуатации, обновления, управление ИТ-активами).

Вопросы информационной безопасности Интернета вещей носят комплексный характер и должны быть решены на всех уровнях архитектуры решения.

Концептуальные документы по архитектурам ведущих платформ Интернета вещей содержат раздел, посвященный безопасности:

− эталонная модель IoT [40];

− The Intel IoT Platform: Architecture Specification White Paper [148];

− Microsoft Azure IoT Reference Architecture [148];

− Industrial Internet Reference Architecture [150];

− и др.

Но в большинстве случаев данный раздел декларирует наиболее общие положения и не содержит практических рекомендаций по обеспечению информационной безопасности.

В то же время для 7 уровневой эталонной модели IoT, опубликованной в 2014 г. Комитетом по архитектуре Всемирного форума IoT, специалистами компании Cisco Systems был разработан фреймворк безопасности IoT, ставший дополнением эталонной модели.

Следует отдельно сказать, что в основе обеспечения информационной безопасности решений IoT в среде облачной платформы Microsoft Azure лежит методика моделирования угроз информационной безопасности STRIDE, рассматривающая все компоненты и уровни решения IoT с точки зрения возникновения различных угроз. Также предлагаются меры и способы противодействию негативным факторам.

Традиционный подход в области информационной безопасности базируется на использовании 3 версии стандарта Common Vulnerability Scoring System (CVSS), который предполагает расчет числового показателя по десятибалльной шкале, на основе которого специалисты по безопасности оперативно принимают решение о том, как реагировать на ту или иную уязвимость и в какой последовательности решать имеющиеся проблемы. Стандарт был разработан группой экспертов по безопасности National Infrastructure Advisory Council.

Российским аналогом перечня угроз можно считать банк данных угроз безопасности информации ФСТЭК РФ (http://bdu.fstec.ru/ubi).

Однако, для облачных технологий в целом, и технологий Интернета вещей данные подходы не всегда применимы или отсутствует наработанная практика применения. Решение данной проблемы актуально. Ощущается отставание в области обеспечения информационной безопасности.

Вопросам совершенствования методической базы в области информационной безопасности Интернета вещей посвящен ряд работ в этой сфере [147].

В таблице 6 представлена классификация типов угроз и мер по их противодействию с учетом уровня архитектуры решения для Интернета вещей. Представленный набор угроз информационной безопасности, конечно же, далеко не полный, но данный набор характеризует концептуальный подход к данному вопросу.

***Таблица 6***

**Типы угроз и меры противодействия для различных уровней архитектуры решения Интернета вещей**

| Уровень архитектуры IoT | Тип угрозы | Меры противодействия |
|---|---|---|
| Уровень восприятия | -подмена оборудования;<br>- внедрение фальшивого узла; | -передача шумовых сигналов в беспроводной сети.<br>-аутентификация; |

| | | |
|---|---|---|
| (Perception Layer) | -внедрение вредоносного кода;<br>-атака на отказ от сна;<br>-подавление сигнала в беспроводной сети | -проверка целостности данных;<br>-безопасная загрузка;<br>-шифрование канала (IPSec);<br>-обезличивание персональных данных;<br>-использование качественных аппаратных компонентов. |
| Сетевой Уровень (Network Layer) | -анализ траффика;<br>-подмена RFID;<br>-неавторизованный доступ RFID;<br>-атака по типу «Ворон ка»;<br>-атака по типу «Человек посередине»;<br>-нарушение маршрутизации | -конфиденциальность данных;<br>-безопасная маршрутизация;<br>-метрики безопасности для передаваемых пакетов;<br>-использование средств геолокации;<br>-механизмы проверки целостности данных. |
| Уровень обработки (Processing Layer) | -нарушение модели безопасности приложений;<br>-несанкционированный доступ к данным;<br>-проблемы безопасности ИТ-инфраструктуры;<br>-проблемы с безопасностью при интеграции компонентов решения;<br>-безопасность для техно логий виртуализации;<br>-безопасность используемых совместно ресурсов. | -обезличивание данных;<br>-шифрование;<br>-сканеры веб-приложе ний;<br>-мониторинг и журналы аудита;<br>-декомпозиция компонентов;<br>-зоны безопасности. |
| Уровень приложений (Application Layer) | - фишинг;<br>-вирусы, черви, шпионское ПО;<br>-вредоносные скрипты;<br>-отказ в обслуживании;<br>-потери данных;<br>-уязвимости программного обеспечения. | -аутентификация;<br>-списки контроля доступа (ACL листы);<br>-антивирусы;<br>-сетевые экраны;<br>-методики оценки риска. |

Источник: [151].

Отдельным направлением для решений Интернета вещей является промышленный Интернет вещей (IIoT), имеющим свои особенности в части обеспечения информационной безопасности.

Существующие подходы к вопросам информационной безопасности промышленного Интернета вещей представлены в таблице 7.

***Таблица 7***

**Подходы к вопросам информационной безопасности промышленного Интернета вещей (IIoT)**

| Наименование инициативы | Разработка вопросов кибер-безопасности | Стандарты и инициативы |
|---|---|---|
| Industrie 4.0 Plattform | Отдельные разделы в рекомендациях по реализации инициатив Industry 4.0 (2013) | Recommendations for implementing the strategic initiative Industrie 4.0 |
| Industrial Internet Consortium (IIC) | Разделы по безопасности референсной Архитектуры Промышленного Интернета. Разработаны на основе стандартов безопасности ИТ и ICS, таких как ENISA, NIST, IEEE, ANSI, ISA, IEC (2015) | Industrial Internet Reference Architecture |
| Open Interconnect Consortium (OIC) | Набор спецификаций, разрабатываемых в качестве приложений к референсной архитектуре интернета вещей (2015) | OIC Specification<br>- Smart Home Device Specification;<br>- Security Specification;<br>- Resource Specification;<br>- Remote Access Specification;<br>- Core Specification. |
| Internet Plus Strategy | Разрабатываются стратегические и прикладные инициативы для каждой критичной отрасли | Practical Application<br>- Internet + Manufacturing Industry;<br>- Internet + Finance;<br>- Internet + Medical System;<br>- Internet + Government;<br>- Internet + Agriculture. |

Основными элементами обеспечения информационной безопасности цифрового пространства Интернета вещей являются идентификация устройства и механизмы аутентификации.

Рассмотренные проблемы безопасности на каждом архитектурном уровне позволяют принять адекватные меры для повышения уровня безопасности решений Интернета вещей, повысить уровень защищенности.

Поскольку решения Интернета вещей станут частью повседневной жизни в ближайшем будущем, то необходимо предпринимать шаги для обеспечения доверия пользователей к данным ИТ и цифровым платформам.

## 2.3. Основные меры противодействия угрозам информационной безопасности

Система обеспечения информационной безопасности АИС должна решать следующие задачи с целью противодействия основным угрозам ИБ [87]:

1. Управление доступом пользователей к ресурсам АИС.

2. Защита данных, передаваемых по каналам связи.

3. Регистрация, сбор, хранение, обработка и выдача сведений обо всех событиях, происходящих в системе и имеющих отношение к ее безопасности.

4. Контроль работы пользователей системы со стороны администрации и оперативное оповещение администратора безопасности о попытках несанкционированного доступа к ресурсам системы.

5. Обеспечение замкнутой среды проверенного программного обеспечения с целью защиты от бесконтрольного внедрения в систему потенциально опасных программ (в которых могут содержаться вредоносные закладки или опасные ошибки) и средств преодоления системы защиты, а также от внедрения и распространения компьютерных вирусов.

6. Контроль и поддержание целостности критичных ресурсов системы защиты; управление средствами защиты.

Различают внешнюю и внутреннюю безопасность АИС. Внешняя безопасность включает защиту АС от стихийных бедствий (пожар, землетрясение и т.п.) и от проникновения в систему злоумышленников извне. Внутренняя безопасность заключается в создании надежных и

удобных механизмов регламентации деятельности всех ее законных пользователей и обслуживающего персонала.

По способам осуществления все меры обеспечения безопасности компьютерных систем подразделяются на: законодательные (правовые), административные (организационные), процедурные и программно-технические.

К законодательным мерам защиты относятся действующие в стране нормативно-правовые акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил. Важное значение имеют стандарты в области защиты информации (в первую очередь, международные). Среди этих стандартов выделяются «Оранжевая книга», рекомендации X.800 и «Общие критерии оценки безопасности ИТ» (Common Criteria for IT Security Evaluation).

«Оранжевая книга» – крупнейший базовый стандарт. В ней даются важнейшие понятия, определяются основные сервисы безопасности и предлагается метод классификации информационных систем по требованиям безопасности.

Рекомендации X.800 в основном посвящены вопросам защиты сетевых конфигураций. Они предлагают развитый набор сервисов и механизмов безопасности.

«Общие критерии» описывают 11 классов, 66 семейств и 135 компонентов функциональных требований безопасности. Классам присвоены следующие названия:

Первая группа определяет элементарные сервисы безопасности:

1. FAU – аудит, безопасность (требования к сервису, протоколирование и аудит);

2. FIA – идентификация и аутентификация;

3. FRU – использование ресурсов (для обеспечения отказоустойчивости).

Вторая группа описывает производные сервисы, реализованные на базе элементарных:

4. FCO – связь (безопасность коммуникаций отправитель-получатель);

5. FPR – приватность;

6. FDP – защита данных пользователя;

7. FPT – защита функций безопасности объекта оценки.

Третья группа классов связана с инфраструктурой объекта оценки:

8. FCS – криптографическая поддержка (обслуживает управление криптоключами и крипто-операциями);

9. FMT – управление безопасностью;

10. FTA – доступ к объекту оценки (управление сеансами работы пользователей);

11. FTP – доверенный маршрут/канал;

Кроме этого «Общие критерии» содержат сведения о том, каким образом могут быть достигнуты цели безопасности при современном уровне ИТ и позволяют сертифицировать систему защиты (ей присваивается определенный уровень безопасности).

Осенью 2006 года в России был принят национальный стандарт ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология – Практические правила управления информационной безопасностью» [41], соответствующий международному стандарту ИСО 17799.

Стандарт представляет собой перечень мер, необходимых для обеспечения информационной безопасности организации, включая действия по созданию и внедрению системы управления информационной безопасности, которая строится таким же образом и на тех же принципах, что и система менеджмента качества, и совместима с ней.

Административные меры защиты – меры организационного характера, регламентирующие процессы функционирования АИС, деятельность персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности. Они включают:

1. Подбор и подготовку персонала системы.

2. Организацию охраны и пропускного режима.

3. Организацию учета, хранения, использования и уничтожения документов и носителей с информацией.

4. Распределение реквизитов разграничения доступа (паролей, ключей шифрования и т.д.).

В составе административных мер защиты важную роль играет формирование программы работ в области информационной безопасности и обеспечение ее выполнения (для этого необходимо выделять необходимые ресурсы и контролировать состояние дел). Основой программы является политика безопасности организации – совокупность руководящих принципов, правил, процедур и практических приёмов в области безопасности, которыми руководствуется организация в своей деятельности. Разработка политики безопасности включает определение следующих основных моментов:

1) какие данные и насколько серьезно необходимо защищать;

2) кто и какой ущерб может нанести организации в информационном аспекте;

3) основные риски и способы их уменьшения до приемлемой величины.

С практической точки зрения политику безопасности можно условно разделить на три уровня: верхний, средний и нижний.

К верхнему уровню относятся решения, затрагивающие организацию в целом (как правило, носят общий характер и исходят от руководства). Например, цели организации в области информационной безопасности, программа работ в области информационной безопасности (с назначением ответственных за ее реализацию).

К среднему уровню относятся вопросы, касающиеся отдельных аспектов информационной безопасности, но важные для различных систем, эксплуатируемых организацией (например, использование на работе персональных ноутбуков, установка непроверенного программного обеспечения, работа с Интернетом и т.д.).

Меры процедурного уровня – отдельные мероприятия, выполняемые на протяжении всего жизненного цикла АИС. Они ориентированы на людей (а не на технические средства) и подразделяются на:

- управление персоналом;
- физическая защита;
- поддержание работоспособности;
- реагирование на нарушения режима безопасности;
- планирование восстановительных работ.

Программно-технические меры защиты основаны на использовании специальных аппаратных средств и программного обеспечения, входящих в состав АИС и выполняющих функции защиты: шифрование, аутентификацию, разграничение доступа к ресурсам, регистрацию событий, поиск и удаление вирусов и т.д. Они будут подробно рассмотрены в следующих главах.

## 2.4. Риски и угрозы информационной безопасности

Несмотря на предпринимаемые дорогостоящие методы, функционирование компьютерных информационных систем выявило наличие слабых мест в защите информации. Неизбежным следствием стали постоянно увеличивающиеся расходы и усилия на защиту информации. Однако для того, чтобы принятые меры оказались эффективными,

необходимо определить, что такое угроза безопасности информации, выявить возможные каналы утечки информации и пути несанкционированного доступа к защищаемым данным.

Подчеркнем, что само понятие «угроза» в разных ситуациях зачастую трактуется по-разному. Например, для подчеркнуто открытой организации угроз конфиденциальности может просто не существовать – вся информация считается общедоступной (СМИ); однако в большинстве случаев нелегальный доступ представляется серьезной опасностью. Иными словами, угрозы, как и все в ИБ, зависят от интересов субъектов информационных отношений (и от того, какой ущерб является для них неприемлемым).

Новые риски и угрозы, возникающие в результате перехода на новые механизмы управления, основанные на широком внедрении современных компьютерных технологий, требуют проведения системных фундаментальных исследований, направленных на выявление этих факторов и выработку механизмов их парирования [108].

Однако, уже сейчас можно с высокой степенью определенности утверждать, что переход к цифровой экономике потребует кардинальных изменений в системе отношений государство – общество – наука – бизнес. В их основу должен быть положен принцип обеспечения максимального доверия. При этом особое внимание должно быть уделено разработке государственной политики, направленной на полноправное вхождение России в число лидирующих стран, и механизмов её реализации, включая законодательное обеспечение, современную систему управления и ее научное сопровождение.

Одной из ключевых проблем массового использования новых технологий является обеспечение безопасности в широком смысле этого слова. Разработка и создание новых технологий фактически привели к замещению биологической среды обитания человека на технологическую. Эти предположения, высказанные писателями-фантастами в середине прошлого века [12], в настоящее время обрели реальные черты. Уже сейчас при принятии решения о массовом внедрении новых технологий, о переходе на новый (постиндустриальный) технологический уклад [88, 89] необходимо руководствоваться положениями экологии технологий, согласно которым технологическое пространство рассматривается как постоянно расширяющаяся часть среды обитания человека. При этом любая, даже самая прогрессивная и социально направленная, технология имеет пределы своего применения, при переходе через которые она может нанести ущерб сопоставимый с положительным эффектом; а применение технологий, не

соответствующих уровню культурного развития (как отдельного человека, так и общества в целом), приводит к катастрофам.

ИКТ-пространство уже сейчас рассматривают как неотъемлемую часть нашей среды обитания. Его особенностями является многофакторное воздействие на общество и людей. Так, собственно информация оказывает влияние на общественное развитие и духовную сферу человека, а средства её отображения, как технические, так и программные, прямо воздействуют на его физическое и психическое состояние [110].

Главной проблемой информационного общества является информационное неравенство, то есть дифференциация пользователей по уровню доступа к информации. Это обусловлено политическими, экономическими, технологическими, субъективными и криминогенными факторами. Выше мы уже рассматривали проблему. Одного процента: разделению богатства между богатейшими людьми (1%) и остальными. Но когда речь идет о доступе к информации эта проблема может иметь еще более сильные последствия, степень которых сейчас до конца не оценена.

Так, например, на политическом уровне дифференциация информации необходима для решения политических задач, задач государственного управления и т.п. Но бесконтрольная централизация информации и ее дифференциация может привести к такой ситуации, когда информационный оператор сможет оказывать прямое несанкционированное воздействие на определенные слои населения (например, электорат).

Экономическая составляющая информационного неравенства зависит от цены как, собственно, информации, так и стоимости её передачи. Поэтому возможности доступа к информации определяется, в том числе, и уровнем платежеспособности. В технологическом плане доступ к информации может быть затруднён отсутствием необходимых систем приёма и передачи информации, техническим возможностями телекоммуникационных систем, не позволяющих обеспечить доставку информации на всю территорию страны [75].

Несовершенство систем защиты информации создаёт угрозы личной безопасности граждан. Например, сбор персональных данных, сведение их в базы данных и последующее неконтролируемое распространение формируют информационную базу деятельности криминальных структур. Кроме того, неконтролируемое использование ИКТ способствует появлению новых видов преступности (терроризм, преступления против личности, в области банковской деятельности и охраны интеллектуальной собственности и др.).

С точки зрения национальной безопасности особую угрозу представляют использование ИКТ в террористических целях,

несанкционированное информационное воздействие на общество, а также на технические системы обеспечения безопасности. В ряде случаев это воздействие, хотя и даёт ярко выраженный отрицательный эффект, но изначально не ставит себе такой цели. В этом плане показательна ситуация с освещением в СМИ и, прежде всего, на телевидении, современных проблем науки. Так, в настоящее время отечественная наука и её достижения не находят адекватного отражения в информационном пространстве. Более того, в обществе посредством ИКТ формируется неадекватное, а порой и негативное отношение к науке [87].

На индивидуальном уровне ИКТ играют роль и как инструмент образовательной деятельности, и как средство труда, и как средство удовлетворения индивидуальных потребностей.

Использование ИКТ в образовании требует кардинального пересмотра подходов к системе воспитания и образования в широком смысле. С одной стороны, образовательные технологии на базе ИКТ позволяют расширить доступ к образовательным услугам, повысить адаптивность и обеспечить непрерывность образования в течение всей жизни. Но при этом наблюдаются такие негативные явления как формирование у детей так называемого «клипового» и «кликового» сознания [125].

Суть этих процессов заключается в том, что ребёнок с детства привыкает простым нажатием кнопки (click) получать информацию в концентрированном виде (clip), но при этом не вырабатываются навыки по её осмыслению и анализу. Следствием этого является утрата творческих начал и формирование стиля поведения, заключающегося в следовании установленным процедурам.

Кроме того, неконтролируемый доступ к виртуальному пространству в детском и юношеском возрасте может привести к такой ситуации, когда будет утеряна грань между действительностью и иллюзиями, сформировано превратное представление об окружающем мире.

Классификация информационных угроз представлена ниже (Рисунок 14, 15).


**Рисунок 14** – Типы информационных угроз

Реализация угроз ИБ заключается в нарушении конфиденциальности, целостности и доступности информации. Злоумышленник может ознакомиться с конфиденциальной информацией, модифицировать ее, или даже уничтожить, а также ограничить или блокировать доступ легального пользователя к информации. При этом злоумышленником может быть как сотрудник организации, так и постороннее лицо. Но, кроме этого, ценность информации может уменьшиться ввиду случайных, неумышленных ошибок персонала, а также сюрпризов, иногда преподносимых самой природой [68].

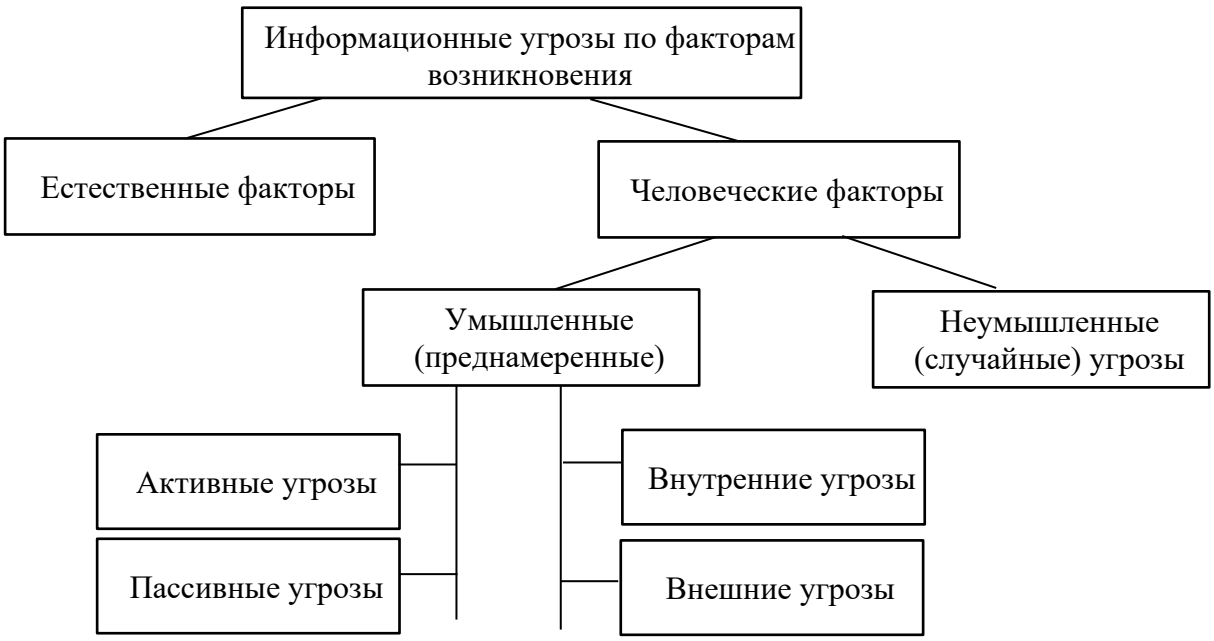



**Рисунок 15** – Классификация информационных угроз по факторам возникновения

Информационные угрозы могут быть обусловлены:

• естественными факторами (стихийные бедствия – пожар, наводнение, ураган, молния и другие причины);

• человеческими факторами. Последние, в свою очередь, подразделяются на:

– угрозы, носящие случайный, неумышленный характер. Это угрозы, связанные с ошибками процесса подготовки, обработки и передачи информации (научно-техническая, коммерческая, валютно-финансовая документация); с нецеленаправленной «утечкой умов», знаний, информации (например, в связи с миграцией населения, выездом в другие страны, для воссоединения с семьей и т.п.) Это угрозы, связанные с ошибками процесса проектирования, разработки и изготовления систем и их компонент (здания, сооружения, помещения, компьютеры, средства связи, операционные системы, прикладные программы и др.) с ошибками в работе аппаратуры из-за некачественного ее изготовления; с ошибками процесса подготовки и обработки информации (ошибки программистов и пользователей из-за недостаточной квалификации и некачественного обслуживания, ошибки операторов при подготовке, вводе и выводе данных, корректировке и обработке информации);

– угрозы, обусловленные умышленными, преднамеренными действиями людей. Это угрозы, связанные с передачей, искажением и уничтожением научных открытий, изобретений секретов производства, новых технологий но корыстным и другим антиобщественным

мотивам (документация, чертежи, описания открытий и изобретений и другие материалы); подслушиванием и передачей служебных и других научно-технических и коммерческих разговоров; с целенаправленной «утечкой умов», знаний информации (например, в связи с получением другого гражданства по корыстным мотивам). Это угрозы, связанные с несанкционированным доступом (НСД) к ресурсам автоматизированной информационной системы (внесение технических изменений в средства вычислительной техники и средства связи, подключение к средствам вычислительной техники и каналам связи, хищение носителей информации: дискет, описаний, распечаток и др.).

Умышленные угрозы преследуют цель нанесения ущерба пользователям АИС и, в свою очередь, подразделяются на активные и пассивные.

Пассивные угрозы, как правило, направлены на несанкционированное использование информационных ресурсов, не оказывая при этом влияния на их функционирование. Пассивной угрозой является, например, попытка получения информации, циркулирующей в каналах связи, посредством их прослушивания.

Активные угрозы имеют целью нарушение нормального процесса функционирования системы посредством целенаправленного воздействия на аппаратные, программные и информационные ресурсы. К активным угрозам относятся, например, разрушение или радиоэлектронное подавление линий связи, вывод из строя ЭВМ или ее операционной системы, искажение сведений в базах данных либо в системной информации и т.д. Источниками активных угроз могут быть непосредственные действия злоумышленников, программные вирусы и т.п.

Умышленные угрозы подразделяются на внутренние, возникающие внутри управляемой организации, и внешние. Внутренние угрозы чаще всего определяются социальной напряженностью и тяжелым моральным климатом. Внешние угрозы могут определяться злонамеренными действиями конкурентов, экономическими условиями и другими причинами (например, стихийными бедствиями).

По данным зарубежных источников, получил широкое распространение промышленный шпионаж – это наносящие ущерб владельцу коммерческой тайны, незаконный сбор, присвоение и передача сведений, составляющих коммерческую тайну, лицом, не уполномоченным на это ее владельцем.

К основным угрозам безопасности относят:

- раскрытие конфиденциальной информации;
- компрометация информации;
- несанкционированное использование информационных ресурсов;

- ошибочное использование ресурсов;
- несанкционированный обмен информацией;
- отказ от информации;
- отказ от обслуживания.

Реализация угроз является следствием одного из следующих действий и событий: разглашения конфиденциальной информации, утечки конфиденциальной информации и НСД к защищаемой информации. При разглашении или утечке происходит нарушение конфиденциальности информации с ограниченным доступом (Рисунок 16).

Средствами реализации угрозы раскрытия конфиденциальной информации могут быть НСД к базам данных, прослушивание каналов и т.п. В любом случае получение информации, являющейся достоянием некоторого лица (группы лиц), что приводит к уменьшению и даже потере ценности информации.


**Рисунок 16** – Действия и события, нарушающие ИБ

Реализацию угроз будем называть атакой.

Утечка конфиденциальной информации — это бесконтрольный выход конфиденциальной информации за пределы ИС или круга лиц, которым она была доверена по службе или стала известна в процессе работы. Эта утечка может быть следствием:

• разглашения конфиденциальной информации;

• ухода информации по различным, главным образом техническим, каналам;

• несанкционированного доступа к конфиденциальной информации различными способами.

Разглашение информации ее владельцем или обладателем есть умышленные или неосторожные действия должностных лиц и пользователей, которым соответствующие сведения в установленном порядке были доверены по службе или по работе, приведшие к ознакомлению с ним лиц, не допущенных к этим сведениям.

Возможна бесконтрольная утечка конфиденциальной информации по визуально-оптическим, акустическим, электромагнитным и другим каналам.

По физической природе возможны следующие средства переноса информации: световые лучи; звуковые волны; электромагнитные волны; материалы и вещества.

Под каналом утечки информации будем понимать физический путь от источника конфиденциальной информации к злоумышленнику, по которому возможна утечка или несанкционированное получение охраняемых сведений. Для возникновения (образования, установления) канала утечки информации необходимы определенные пространственные, энергетические и временные условия, а также соответствующие средства восприятия и фиксации информации на стороне злоумышленника.

Применительно к практике с учетом физической природы образования каналы утечки информации можно разделить на следующие группы:

• визуально-оптические;

• акустические (включая и акустико-преобразовательные);

• электромагнитные (включая магнитные и электрические);

• материально-вещественные (бумага, фото, магнитные носители, производственные отходы различного вида - твердые, жидкие, газообразные).

НСД – это наиболее распространенный вид информационных угроз заключается в получении пользователем доступа к объекту, на

который у него нет разрешения в соответствии с принятой в организации политикой безопасности. Обычно самая главная проблема определить, кто и к каким наборам данных должен иметь доступ, а кто нет.

По характеру, воздействия НСД является активным воздействием, использующим ошибки системы. НСД обращается обычно непосредственно к требуемому набору данных, либо воздействует на информацию о санкционированном доступе с целью легализации НСД. НСД может быть подвержен любой объект системы. НСД может быть осуществлен как стандартными, так и специально разработанными программными средствами к объектам.

Есть и достаточно примитивные пути НСД:

- хищение носителей информации и документальных отходов;
- инициативное сотрудничество;
- склонение к сотрудничеству со стороны взломщика;
- выпытывание;
- подслушивание;
- наблюдение и другие пути.

Любые способы утечки конфиденциальной информации могут привести к значительному материальному и моральному ущербу как для организации, где функционирует ИС, так и для ее пользователей.

Разглашение и утечка приводит к неправомерному ознакомлению с конфиденциальной информацией при минимальных затратах усилий со стороны злоумышленника. Этому способствуют некоторые не лучшие личностно-профессиональные характеристики и действия сотрудников фирмы, представленные на рисунке 17.

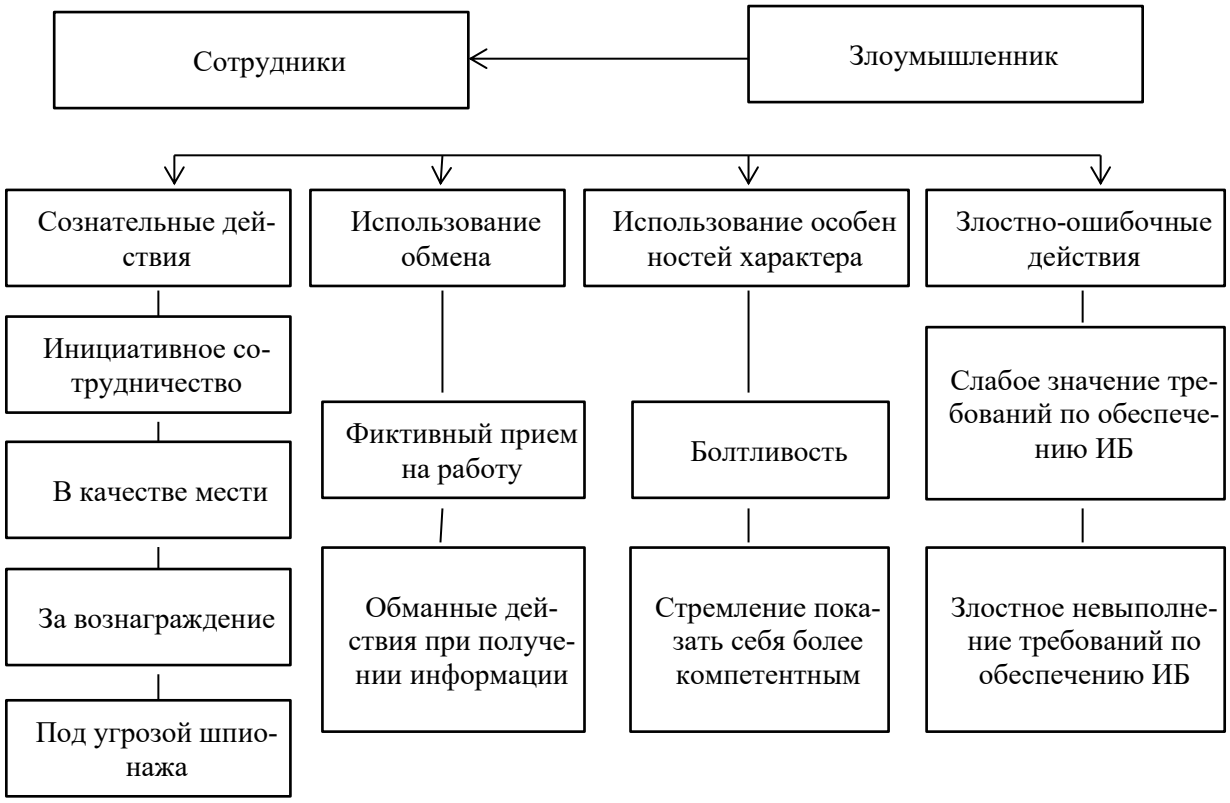



**Рисунок 17** – Личностно-профессиональные характеристики и действия сотрудников, способствующие реализации угроз ИБ

Обиженные сотрудники, даже бывшие, знакомы с порядками в организации и способны нанести немалый ущерб. Необходимо следить за тем, чтобы при увольнении сотрудника его права доступа (логического и физического) к информационным ресурсам аннулировались. Типы и субъекты информационных угроз представлены в таблице 8.

***Таблица 8***

**Типы и субъекты угроз**

| № | Тип угроз | Оператор | Руководитель | Программист | Инженер (техник) | Пользователь | Конкурент |
|---|---|---|---|---|---|---|---|
| 1. | Изменение кодов | + | | + | | | |
| 2. | Копирование файлов | + | | + | | | |
| 3. | Уничтожение файлов | + | + | + | | + | + |
| 4. | Присвоение программ | | | + | + | | + |
| 5. | Шпионаж | + | + | + | | | + |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 6. | Установка подслушивания | | | + | + | | + |
| 7. | Саботаж | + | | + | + | | + |
| 8. | Продажа данных | + | + | + | | + | |
| 9. | Воровство | | + | + | | + | + |

И даже если сотрудник не является злоумышленником, он может ошибаться не намеренно вследствие усталости, болезненного состояния и пр.

Ошибочное использование информационных ресурсов, будучи санкционированным, тем не менее, может привести к разрушению, раскрытию или компрометации указанных ресурсов. Данная угроза, чаще всего, является следствием ошибок в программном обеспечении АИС.

Уничтожение компьютерной информации – это стирание ее в памяти ЭВМ, удаление с физических носителей, а также несанкционированные изменения составляющих ее данных, кардинально меняющие содержание (например, введение ложной информации, добавление, изменение, удаление записей). Одновременный перевод информации на другой машинный носитель не считается в контексте уголовного закона уничтожением компьютерной информации лишь в том случае, если в результате этих действий доступ правомерных пользователей к информации не оказался существенно затруднен либо исключен.

Имеющаяся у пользователя возможность восстановить уничтоженную информацию с помощью средств программного обеспечения или получить данную информацию от другого пользователя не освобождает виновного от ответственности.

Уничтожением информации не является переименование файла, где она содержится, а также само по себе автоматическое "вытеснение" старых версий файлов последними по времени.

Блокирование компьютерной информации – это искусственное затруднение доступа пользователей к компьютерной информации, не связанное с ее уничтожением. Другими словами, это совершение с информацией действий, результатом которых является невозможность получения или использование ее по назначению при полной сохранности самой информации.

Компрометация информации, как правило, реализуется посредством внесения несанкционированных изменений в базы данных, в

результате чего ее потребитель вынужден либо отказаться от нее, либо предпринимать дополнительные усилия для выявления изменений и восстановления истинных сведений. В случае использования скомпрометированной информации потребитель подвергается опасности принятия неверных решений со всеми вытекающими последствиями.

Отказ от информации, в частности, непризнание транзакции (операции в банке) состоит в непризнании получателем или отправителем информации фактов ее получения или отправки. В условиях маркетинговой деятельности это, в частности, позволяет одной из сторон расторгать заключенные финансовые соглашения «техническим» путем, формально не отказываясь от них и нанося тем самым второй стороне значительный ущерб.

Копирование компьютерной информации – изготовление и устойчивое запечатление второго и последующих экземпляров базы данных, файлов в любой материальной форме, а также их запись на машинный носитель, в память ЭВМ.

Отказ в обслуживании представляет собой весьма существенную и распространенную угрозу, источником которой является сама АИС. Подобный отказ особенно опасен в ситуациях, когда задержка с предоставлением ресурсов абоненту может привести к тяжелым для него последствиям. Так, отсутствие у пользователя данных, необходимых для принятия решения, в течение периода, когда это решение еще может быть эффективно реализовано, может стать причиной его нерациональных действий.

Ниже перечисляются наиболее распространенные технические угрозы и причины, в результате которых они реализуются:

• НСД к информационной системе - происходит в результате получения нелегальным пользователем доступа к информационной системе;

• раскрытие данных – наступает в результате получения доступа к информации или ее чтения человеком и возможного раскрытия им информации случайным или намеренным образом;

• несанкционированная модификация данных и программ – возможна в результате модификации, удаления или разрушения человеком данных и программного обеспечения локальных вычислительных сетей случайным или намеренным образом;

• раскрытие трафика локальных вычислительных сетей – произойдет в результате доступа к информации или ее чтения человеком и возможного ее разглашения случайным или намеренным образом

тогда, когда информация передается через локальные вычислительные сети;

• подмена трафика локальных вычислительных сетей – это его использование легальным способом, когда появляются сообщения, имеющие такой вид, будто они посланы законным заявленным отправителем, а на самом деле это не так;

• неработоспособность локальных вычислительных сетей – это следствие осуществления угроз, которые не позволяют ресурсам локальных вычислительных сетей быть своевременно доступными.

Непосредственный вред от реализованной угрозы называется воздействием угрозы.

Угрозы, исходящие от окружающей среды, весьма разнообразны. В первую очередь следует выделить нарушение инфраструктуры – аварии электропитания, временное отсутствие связи, перебои с водоснабжением, гражданские беспорядки и т. п. На долю огня, воды и аналогичных «врагов», среди которых самый опасный – низкое качество электропитания, приходится 13% потерь, которые обычно несут информационные системы.

Внешние субъекты могут быть случайными или преднамеренными и иметь разный уровень квалификации. К ним относятся:

• криминальные структуры;

• потенциальные преступники и хакеры;

• недобросовестные партнеры;

• технический персонал поставщиков услуг;

• представители надзорных организаций и аварийных служб;

• представители силовых структур.

Внутренние субъекты, как правило, представляют собой высококвалифицированных специалистов в области разработки и эксплуатации программного обеспечения и технических средств, знакомы со спецификой решаемых задач, структурой и основными функциями и принципами работы программно-аппаратных средств защиты информации, имеют возможность использования штатного оборудования и технических средств сети. К ним относятся:

• основной персонал (пользователи, программисты, разработчики);

• представители службы защиты информации;

• вспомогательный персонал (уборщики, охрана);

• технический персонал (жизнеобеспечение, эксплуатация).

Технические средства, являющиеся источниками потенциальных угроз безопасности информации, также могут быть внешними:

средства связи; сети инженерных коммуникаций (водоснабжения, канализации); транспорт.

При взаимодействии интегрированной информационной системы управления предприятием с Internet основные угрозы для ИБ организации представляют:

• несанкционированные внешние воздействия из Internet на информационную систему для получения доступа к ее ресурсам и (или) нарушения ее работоспособности;

• отказы аппаратного и программного обеспечения подсистемы взаимодействия (нарушение работы каналов связи с Internet, телекоммуникационного оборудования локальной вычислительной сети, межсетевых экранов);

• непреднамеренные действия сотрудников организации, приводящие к непроизводительным затратам времени и ресурсов, разглашение сведений ограниченного пользования через Internet или нарушению работоспособности подсистемы взаимодействия интегрированной информационной системы управления предприятием с Internet;

• преднамеренные действия сотрудников организации, приводящие к разглашению сведений ограниченного пользования через Internet, а также нарушение работоспособности подсистемы взаимодействия информационной системы с Internet или же недоступность предоставляемых услуг через Internet;

• непреднамеренные действия лиц, осуществляющих администрирование подсистемы взаимодействия интегрированной информационной системы управления предприятием с Internet, приводящие к разглашению сведений ограниченного пользования или нарушению взаимодействия с Internet;

• преднамеренные действия (в корыстных целях, по принуждению третьих лиц, со злым умыслом и т.п.) сотрудников организации, отвечающих за установку, сопровождение, администрирование системного, сетевого или прикладного программного обеспечения, технических средств защиты и обеспечения ИБ подсистемы взаимодействия интегрированной информационной системы управления предприятием с Internet, которые (действия) приводят к разглашению сведений ограниченного пользования или нарушения взаимодействия с Internet.

Угрозы безопасности можно классифицировать по следующим признакам:

1. По цели реализации угрозы. Реализация той или иной угрозы безопасности может преследовать следующие цели:

- нарушение конфиденциальной информации;

- нарушение целостности информации;

- нарушение (частичное или полное) работоспособности.

2. По принципу воздействия на объект:

- с использованием доступа субъекта системы (пользователя, процесса) к объекту (файлам данных, каналу связи и т.д.);

- с использованием скрытых каналов.

Под скрытым каналом понимается путь передачи информации, позволяющий двум взаимодействующим процессам обмениваться информацией таким способом, который нарушает системную политику безопасности.

3. По характеру воздействия на объект.

По этому критерию различают активное и пассивное воздействие.

Активное воздействие всегда связано с выполнением пользователем каких-либо действий, выходящих за рамки его обязанностей и нарушающих существующую политику безопасности. Это может быть доступ к определенным наборам данных, программам, вскрытие пароля и т.д. Активное воздействие ведет к изменению состояния системы и может осуществляться либо с использованием доступа (например, к наборам данных), либо как с использованием доступа, так и с использованием скрытых каналов.

Пассивное воздействие осуществляется путем наблюдения пользователем каких-либо побочных эффектов (от работы программы, например) и их анализе. На основе такого рода анализа можно иногда получить довольно интересную информацию. Примером пассивного воздействия может служить прослушивание линии связи между двумя узлами сети. Пассивное воздействие всегда связано только с нарушением конфиденциальности информации, так как при нем никаких действий с объектами и субъектами не производится. Пассивное воздействие не ведет к изменению состояния системы.

4. По причине появления используемой ошибки защиты.

Реализация любой угрозы возможна только в том случае, если в данной конкретной системе есть какая-либо ошибка или брешь защиты.

Такая ошибка может быть обусловлена одной из следующих причин:

- неадекватностью политики безопасности реальной системе. Это означает, что разработанная политика безопасности настолько не отражает реальные аспекты обработки информации, что становится

возможным использование этого несоответствия для выполнения несанкционированных действий;

- ошибками административного управления, под которыми понимается некорректная реализация или поддержка принятой политики безопасности в данной организации. Например, согласно политике безопасности должен быть запрещен доступ пользователей к определенному набору данных, а на самом деле (по невнимательности администратора безопасности) этот набор данных доступен всем пользователям.

- ошибками в алгоритмах программ, в связях между ними и т.д., которые возникают на этапе проектирования программы или комплекса программ и благодаря которым их можно использовать совсем не так, как описано в документации. Примером такой ошибки может служить ошибка в программе аутентификации пользователя, когда при помощи определенных действий пользователь имеет возможность войти в систему без пароля.

- ошибками реализации алгоритмов программ (ошибки кодирования), связей между ними и т.д., которые возникают на этапе реализации или отладки и которые также могут служить источником недокументированных свойств.

5. По способу воздействия на объект атаки (при активном воздействии):

- непосредственное воздействие на объект атаки (в том числе с использованием привилегий), например, непосредственный доступ к набору данных, программе, службе, каналу связи и т.д., воспользовавшись какой-либо ошибкой. Такие действия обычно легко предотвратить с помощью средств контроля доступа.

- воздействие на систему разрешений (в том числе захват привилегий). При этом способе НСД выполняются относительно прав пользователей на объект атаки, а сам доступ к объекту осуществляется потом законным образом.

Примером может служить захват привилегий, что позволяет затем беспрепятственно получить доступ к любому набору данных и программе, в частности «маскарад», при котором пользователь присваивает себе каким-либо образом полномочия другого пользователя выдавая себя за него.

6. По объекту атаки. Одной из самых главных составляющих нарушения функционирования АИС является объект атаки, т.е. компонент системы, который подвергается воздействию со стороны злоумышленника. Определение объекта атаки позволяет принять меры по

ликвидации последствий нарушения, восстановлению этого компонента, установке контроля по предупреждению повторных нарушений и т.д.

Воздействию могут подвергаться следующие компоненты:

- АИС в целом – злоумышленник пытается проникнуть в систему для последующего выполнения каких-либо несанкционированных действий. Для этого обычно используются метод «маскарада», перехват или подделка пароля, взлом или доступ к системе через сеть;

- объекты системы – данные или программы в оперативной памяти или на внешних носителях, сами устройства системы, как внешние (дисководы, сетевые устройства, терминалы), так и внутренние (оперативная память, процессор), каналы передачи данных. Воздействие на объекты системы обычно имеет целью доступ к их содержимому (нарушение конфиденциальности или целостности обрабатываемой или хранимой информации) или нарушение их функциональности, например, заполнение всей оперативной памяти компьютера бессмысленной информацией или загрузка процессора компьютера задачей с неограниченным временем исполнения (нарушение доступности);

- субъекты системы – процессы и подпроцессы с участием пользователей. Целью таких атак является либо прямое воздействие на работу процесса – его приостановка, изменение привилегий или характеристик (приоритета, например), либо обратное воздействие - использование злоумышленником привилегий, характеристик и т.д. другого процесса в своих целях. Частным случаем такого воздействия является внедрение злоумышленником вируса в среду другого процесса и его выполнение от имени этого процесса. Воздействие может осуществляться на процессы пользователей, системы, сети;

- каналы передачи данных - пакеты данных, передаваемые по каналу связи и сами каналы. Воздействие на пакеты данных может рассматриваться как атака на объекты сети, воздействие на каналы – специфический род атак, характерный для сети. К нему относятся: прослушивание канала и анализ трафика (потока сообщений) – нарушение конфиденциальности передаваемой информации; подмена или модификация сообщений в каналах связи и на узлах ретрансляторах – нарушение целостности передаваемой информации; изменение топологии и характеристик сети, правил коммутации и адресации

- нарушение доступности сети.

7. По используемым средствам атаки.

Для воздействия на систему злоумышленник может использовать стандартное программное обеспечение или специально разработанные

программы. В первом случае результаты воздействия обычно предсказуемы, так как большинство стандартных программ системы хорошо изучены. Использование специально разработанных программ связано с большими трудностями, но может быть более опасным, поэтому в защищенных системах рекомендуется не допускать добавление программ в АИС экономических объектов без разрешения администратора безопасности системы.

Развитие ИТ подталкивает нас в сфере знаний к полной зависимости от техники. Избыточность информации вокруг создает иллюзию ее постоянной достаточности. Из «внутреннего» знание постепенно становится «внешним». Мозг человека уже более не является единственным хранилищем информации и носителем знаний [82].

Таким образом, человек добровольно превращает собственную память в атавизм. При этом человек теряет индивидуальность информационного пространства. Современные гаджеты позволяют фиксировать и неконтролируемо распространять любые, даже самые закрытые, подробности о его личной жизни [15].

Таким образом, на повестку дня выходит вопрос планирования и экспертизы технологий уже на стадии их создания, а также контроля применения технологий с целью минимизации возможных негативных последствий.

# ЗАКЛЮЧЕНИЕ

Результаты выполненных исследований показали актуальность и своевременность для российской экономики рассматриваемых вопросов в области цифровой экономики.

В работе значительное внимание уделено вопросам, связанным с рассмотрением сути цифровой экономики, причин ее возникновения, нормативного и правового регулирования, а также показана важность информационной инфраструктуры при формировании цифровой экономики и информационной безопасности при ее развитии.

В целом, работа отражает научные взгляды на современное состояние и развитие экономики в условиях цифровизации. Она представляет интерес как для специалистов в области проведения научных исследований, так и специалистов-практиков.

## Использованная литература:


1. Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы». URL: http://www.garant.ru/products/ipo/prime/ doc/ 71570570/ (дата обращения: 19.07.2020). – Текст: электронный.
2. Указ Президента РФ от 01.12.2016 № 642 «О Стратегии научно-технологического развития Российской Федерации» // Консультант Плюс. – URL: http://www.consultant.ru/document/ cons_doc_ LAW_207967/ (дата обращения: 06.08.2020). – Текст: электронный.
3. Аверьянов, М. А. Государство и экономика: новые цифровые возможности / М.А. Аверьянов, С.Н. Евтушенко, Е.Ю. Кочетова // Экон. стратегии. – 2017. – Т.19, №5 (147). – С. 106–113.
4. Агеев, А. И. Формирование организационных и информационных механизмов управления построением в России цифровой экономики / А.И. Агеев, Е.Л. Логинов // Экон. стратегии. – 2018. – №3 (153). – С. 56–67.
5. Аналитический отчет IOT Analytics: IoT security market report 2017-2022. – URL: https://iot-analytics.com/ (дата обращения: 12.09.2020). – Текст: электронный.
6. Андиева, Е. Ю. Цифровая экономика будущего, индустрия 4.0 / Е.Ю. Андиева, В.Д. Фильчакова // Прикладная математика и фундамент. информатика. – Омск, 2016. – №3. – С. 214–218.
7. Аполов, О. Г. От «цифровизации» к «цифровой экономике» / О. Г. Аполов, О. А. Зыков, О. О. Аполова // Экономика и предпринимательство. – 2018. – №4 (93). – С. 73–77.
8. Асадуллина, А. В. Цифровая экономика в России: текущий статус и проблемы развития / А. В. Асадуллина // Рос. внешнеэкон. вестн. – 2018. – №6. – С. 98–112.
9. Асанов, Р. К. Формирование концепции «цифровой экономики» в современной науке / Р. К. Асанов // Социально-экономические науки и гуманитарные исследования. – 2016. – № 15. – С. 143–148.
10. Бабаев, Д. Б. К вопросу о развитии экономики информационного общества: авторское понятие «экономики идей» / Д. Б. Бабаев, Е. Д. Бабаев // Соврем. наукоемкие технологии. Регион. прил. – 2016. – №1 (45). – С. 9–15.
11. Байнев, В. Ф. Четвертая промышленная революция как очередной этап экономической интеграции / В. Ф. Байнев // Экономист. – 2017. – № 2. – С. 3–9

12. Балагаев, А. Ю. Цифровая трансформация экономики России: возможности и риски / А. Ю. Балагаев // Банковское дело. – 2018. – №7. – С. 64–67.

13. Барабаш, К. С. Влияние цифровой экономики на изменение рынка труда / К. С. Барабаш // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. – 2018. – №6 (97). – С. 52–54.

14. Бархатов, В. И. Мировой опыт развития цифровой экономики. Перспективы перехода в России / В. И. Бархатов, С. В. Лушников, Д. С. Бенц // Друкеровский вестн. – 2018. – №2 (22). – С.19–26.

15. Башина, О. Э. Трансформация экономической и трудовой модели поведения современной молодежи в условиях становления цифрового общества / О. Э. Башина, Е. С. Васютина, Л. В. Матраева // Знание. Понимание. Умение. – 2018. – №3. – С.133–145.

16. Бойко, И. П. Экономика предприятия в цифровую эпоху / И. П. Бойко, М. А. Евневич, А. В. Колышкин // Российское предпринимательство. – 2017. – Том 18. – № 7. – С. 1127–1136.

17. Бондаренко, В. М. Мировоззренческий подход к формированию, развитию и реализации «цифровой экономики» / В. М. Бондаренко // Современные информационные технологии и ИТ-образование. – 2017. – № 1, Т. 13. – С. 237–251.

18. Бренделева, Е. А. Человеческий капитал в цифровой экономике / Е. А. Бренделева // Экономика и управление: проблемы, решения. – М., 2018. – №6, т.1. – С.161–166.

19. Будзинская, О. В. Структура занятости российского рынка труда в условиях перехода к цифровой экономике / О. В. Будзинская, А. Э. Славинский, А. А. Туманов // Проблемы экономики и упр. нефтегазовым комплексом. – 2018. – №6. – С. 39–43.

20. Бухт, Р. Определение, концепция и измерение цифровой экономики / Р. Бухт, Р. Хикс // Вестник международных организаций. – 2018. – № 2, Т. 13. – С. 143–172.

21. Владимирова, Ц. Д. Развитие теории человеческого капитала организаций в цифровой экономике / Ц. Д. Владимирова // Рос. предпринимательство. 2018. – Т.19, № 9. – С. 2671–2690.

22. Володин, В. М. Влияние цифровой экономики на трансформацию человеческого капитала / В. М. Володин, И. А. Питайкина, С. А. Влазнева // Экон. науки. – 2018. – №6 (163). – С. 44–48.

23. Воробьев, Ю. Н. Становление цифровой экономики в России и ее влияние на социальную сферу / Ю. Н. Воробьев, Е. И. Воробьева // Экономика и предпринимательство. – 2018. – №4 (93). – С. 78–86.

24. Гасанов, Г. А. Цифровая экономика как новое направление экономической теории / Г. А. Гасанов, Т. А. Гасанов // Региональные проблемы преобразования экономики. – 2017. – № 6(80). – С. 4–10.

25. Гейтс, Б. Бизнес со скоростью мысли. – М.: Эксмо-Пресс, 2000.

26. Гербина Т. Цифровая экономика – новая мировая реальность / Т. Гербина // Вестн. Моск. междунар. акад. – 2018. – №1 (13). – С. 92–113.

27. Головенчик, Г. Г. Цифровизация белорусской экономики в современных условиях глобализации / Г. Г. Головенчик. – Минск : Изд. центр БГУ, 2019. – 257 с. – ISBN 978-985-553-581-3.

28. Городов, О. А. Основные направления совершенствования правового регулирования в сфере цифровой экономики в России / О. А. Гордов, М. А. Егорова // Право и цифровая экономика. – 2018. – №1 (1). – С. 6–12

29. Гретченко, А. И. Закономерности эволюции цифровой экономики и перспективы ее развития в России / А. И. Гретченко // Наука и практика: науч.-аналит. журн. Рос. экон. ун-та им. Г. В. Плеханова. – 2018. – №2 (30). – С. 28–36.

30. Гретченко, А. И. Формирование цифровой экономики в России / А. И. Гретченко, И. В. Горохова, А. А. Гретченко // Вестн. Рос. экон. ун-та им. Г.В. Плеханова. – 2018. – №3 (99). – С. 3–11.

31. Дадалко, В. А. Компетенции для цифровой экономики и трансформация образовательной системы в условиях VI экономического уклада / В. А. Дадалко, Е. Д. Соловкина // Нац. интересы: приоритеты и безопасность. – 2018. – Т.14, №5. – С. 913–926.

32. Демьянова, О. Влияние цифровизации на кадровую политику / О. Демьянова, Э. Ахметшина // Проблемы теории и практики упр. – 2018. – №4. – С. 117–122.

33. Добрынин, А. П. Цифровая экономика – различные пути к эффективному применению технологий / А. П. Добрынин, К. Ю. Черних, В. П. Куприяновский // International Journal of Open Information Technologies. – 2016. – №1 (4). – С. 4–10.

34. Дравица, В. Промышленная революция Industry 4.0 / В. Дравица, А. Курбацкий // Наука и инновации. – 2016. – № 3. – С. 13–16.

35. Дятлов, С. А. Сетевая занятость и сетевая безработица в цифровой экономике / С. А. Дятлов // Экономика и управление: проблемы, решения. – 2018. – №4, т.4. – С. 145–152.

36. Егозарьян, В. В. «Цифра» как точка опоры / В. В. Егозарьян, Э. В. Маймина // Вестн. Белгород. ун-та кооперации, экономики и права. – 2018. – №1 (68). – С. 116–131.

37. Заседание Совета по стратегическому развитию и приоритетным проектам : официальный сайт Президента России. – URL: http://

kremlin.ru/events/president/transcripts/54983 (дата обращения: 07.07.2020). – Текст: электронный.

38. Зонова, Н. С. Роль цифровой экономики в реформировании российского общества / Н. С. Зонова // Образование и наука в современных реалиях: материалы II Междунар. науч.-практ. конф. (Чебоксары, 5 нояб. 2017 г.) / редкол.: О. Н. Широков [и др.]. – Чебоксары: ЦНС «Интерактив плюс», 2017. – С. 296–298.

39. Инициатива «Группы двадцати» по развитию и сотрудничеству в области цифровой экономики // Сайт Президента России. – URL: http://kremlin.ru/supplement/5111 (дата обращения: 18.10.2020). – Текст: электронный.

40. Интернет вещей: сетевая архитектура и архитектура безопасности // Информационный сборник «Интернет изнутри». – URL: http://internetinside.ru/internet-veshhey-setevaya-arkhitektura-i/ (дата обращения: 28.05.2020). – Текст: электронный.

41. Информационная технология. Практические правила управления информационной безопасностью / ГОСТ Р ИСО/МЭК 17799-2005. – URL: http://docs.cntd.ru/document/gost-r-iso-mek-17799-2005 (дата обращения: 08.06.2020). – Текст: электронный.

42. Калужский, М. Л. Электронная коммерция: маркетинговые сети и инфраструктура рынка / М. Л. Калужский; ОмГТУ. – М.: Экономика, 2014. – 328 с.

43. Каржина, А. А. Направления развития цифровой экономики: проблемы и перспективы / А. А. Каржина // Актуальные проблемы управления, экономики и права: научные подходы студентов и аспирантов. Право и экономика: сб. науч. работ. – 2018. – С. 313–322.

44. Кастельс, М. Информационная эпоха: экономика, общество и культура / М. Кастельс. – М.: ГУ ВШЭ, 2000. – 608 с.

45. Кауфман, Н. Ю. Трансформация управления знаниями в условиях развития цифровой экономики / Н. Ю. Кауфман // Креативная экономика. – 2018. – Т.12, №3. – С. 261–270

46. Кибер-безопасность: человеческий фактор, 12.06.2018. – URL: https://legal-it.club/kiberbezopasnost-chelovecheskij-faktor (дата обращения: 31.07.2020). – Текст: электронный.

47. Киселев, М. И. Цифровая экономика и четвертая промышленная революция – новые вызовы или дань времени? / М. И. Киселев, А. С. Комшин, А. Б. Сырицкий // Стандарты и качество. – 2018. – №4. – С. 62–66.

48. Кисляков, П. А. Цифровой гендерный разрыв как фактор риска социальной безопасности российского общества / П. А. Кисляков, Е. А. Шмелева // Женщина в рос. обществе. – 2018. – № 3. – С. 14–25.

49. Клейнер, Г. Б. Человек в цифровой экономике / Г. Б. Клейнер, Ю. А. Кораблев, С. Е. Щепетова // Экон. наука соврем. России. – 2018. – №2. – С. 169–175.

50. Клименков, Г. В. Программа цифровой экономики – пути реализации / Г. В. Клименков // Вестн. Пермского нац.- исслед. политехн. ун-та. – 2018. – №2. – С. 127–136.

51. Коба, Е. Е. Проблемы интеграции цифровой экономики / Е.Е. Коба // Перспективы, организационные формы и эффективность развития сотрудничества российских и зарубежных ВУЗов: сборник материалов VI Междунар. науч.-практ. конф., 12-13 апреля 2018 г. – Королёв (Моск. обл.), 2018. – С. 285–297.

52. Колодняя, Г. В. Преимущества и риски цифровой экономики / Г.В. Колодняя // Философия хозяйства: материалы Междунар. науч. конф. «Институциональные и финансовые механизмы становления цифровой экономики», 17-18 ноября 2017 г. – М., 2017. – С. 24–33.

53. Колпакова, Г. М. Анализ факторов формирования информационной экономики в условиях глобализации / Г.М. Колпакова, Ю.В. Евдокимова // Аудит и финн. анализ. – М., 2016. – №5. – С. 403–407

54. Комаров, О. К. Развитие трудовых отношений в информационной экономике / О. К. Комаров // Вестн. Поволж. ин-та упр. – Саратов, 2016. – №2 (53). – С. 13–18.

55. Комаров, А. В. Прогнозирование экономического развития России до 2025 года в условиях становления цифровой экономики / А. В. Комаров, Е. С. Борисова, Э. Р. Кузбенова // Экономика и предпринимательство. – М., 2018. – №3 (92). – С. 88–97.

56. Кондрашов, В. М. Человеческий капитал и цифровая экономика: региональный аспект / В. М. Кондрашов, А. В. Мосийчук, М. В. Шеломенцева // Регион. проблемы преобразования экономики. – Махачкала, 2017. – №12 (86). – С.77–82.

57. Коровникова, Н. А. Рынок труда и цифровая экономика: тенденции и перспективы / Н. А. Коровникова // Экон. и социал. проблемы России. – М., 2018. – №1 (37). – С.96–110.

58. Красильникова, Е. В. Системные признаки интернет-экономики / Е. В. Красильникова // Известия Саратовского университета. Серия: Экономика. Управление. Право. – 2011. – Т. 11, № 1. – С. 32–37.

59. Креативная экономика – двигатель и катализатор устойчивого развития / Центр новостей ООН // Официальный сайт ООН. – URL: https://news.un.org/ru/story/2013/ 11/1232591. (дата обращения: 17.10.2020). – Текст: электронный.

60. Крутиков, В. К. Цифровая экономика: проблемы и возможности: монография / В. К. Крутиков. – Калуга: Политоп, 2018. – 179 с.

61. Куксова, О. Д. Изменение условий занятости в информационной экономике как фактор трансформации среднего класса / О. Д. Куксова // Экономика и предпринимательство. – М., 2016. – №12 (77), ч.2. – С.174–177.

62. Кунцман, А. А. Трансформация внутренней и внешней среды бизнеса в условиях цифровой экономики / А. А. Кунцман // Управление экономическими системами: электронный научный журнал. – 2016. – № 11(93). – С. 1–11.

63. Курылев, К. Л. Цифровая зависимость НАТО / К. Л. Курылев, В. Т. Цаканян // Вестник Московского государственного областного университета. Серия: История и политические науки. – 2018. − №1. − С. 45–51.

64. Лебедев, В. А. Невиртуальная реальность цифровой экономики / В. А. Лебедев, Е. И. Лебедева // Бух. учет и налогообложение в бюджетных орг. – М., 2017. – №10. – С. 59–63.

65. Лезина, Т. А. Анализ требований работодателей к цифровым компетенциям сотрудников / Т. А. Лезина, А. Д. Юркова // Рос. предпринимательство. – М., 2018. – Т.19, №5. – С. 1623–1632.

66. Лопатин, В. Н. Проблемы информационной безопасности и риски интеллектуальной собственности в цифровой экономике / В. Н. Лопатин // Информ. право. – М., 2017. – №2. – С. 8–16.

67. Лопатин, В. Н. Риски информационной безопасности при переходе к цифровой экономике / В. Н. Лопатин // Государство и право. – М., 2018. – №3. – С. 77–88.

68. Мавлютова, Г. А. Устойчивое развитие цифровой экономики как элемент обеспечения национальной безопасности Российской Федерации / Г. А. Мавлютова, Е. Б. Ножкина, П. Л. Алтухов // Экон. безопасность и качество. – Саратов, 2018. – №1 (30). – С.19–24.

69. Макаров, В. Л. Контуры экономики знаний / В. Л. Макаров // Экономист. – 2003. – № 3. – С. 3–15.

70. Максакова, М. А. Цифровая трансформация экономики: опыт передовых стран / М. А. Максакова // Экономика и управление: проблемы, решения. – М., 2018. – №4, т.5. – С. 5–8.

71. Максютина, Е. В. Социальные проблемы и вызовы цифровой экономики / Е. В. Максютина, А. В. Головкин // Четвертая промышленная революция: реалии и современные вызовы : сб. материалов междунар. науч. конф. X юбилейные Санкт-Петербургские социологические чтения, 13-14 апреля 2018 года, Санкт-Петербург. – СПб., 2018. – С. 70–74.

72. Манахова, И. В. Потребление в информационной экономике XXI века: монография / И. В. Манахова. – М.: МАКС Пресс, 2014. – 286 с.

73. Манахова, И. В. Цифровое будущее и глобальная экономическая безопасность / И. В. Манахова // Экон. безопасность и качество. – Саратов, 2018. – №1 (30). – С. 6–11.

74. Марьина, Е. Ю. Цифровое пространство: противоречия становления и развития // Young Scientist. – № 9(36). – september 2016. – С. 335–338. – URL: http://molodyvcheny.in.ua/files/journal/2016/9/116.pdf (дата обращения: 15.06.2020). – Текст: электронный.

75. Масленникова, Ю. Л. Цифровое неравенство как социальный фактор цифровой экономики / Ю. Л. Масленникова, А. А. Давыдова // Экономика и предпринимательство. – М., 2018. – №3 (92). – С. 953–956.

76. Маханьков, Н. Г. Креативная экономика / Н. Г. Маханьков, М. А. Дроздов, Н. Д. Корсукова // Актуальные проблемы авиации и космонавтики. – 2015. – Т. 2, № 11. – С. 585–586

77. Нежметдинова, Ф. Т. Трансформация образования в условиях формирования цифровой экономики / Ф. Т. Нежметдинова, Н. С. Барабаш // Инноватика и экспертиза: науч. тр. – М., 2018. – №2 (23). – С. 120–131.

78. Новая парадигма общественного развития в условиях цифровой экономики: монография / Н. В. Угрюмова, А. А. Копченов, О. В. Перевозова и др.; Фин. ун-т при Правительстве Рос. Федерации (Челяб. фил.). – Челябинск: Челяб. Дом печати, 2018. – 123 с.

79. Носова, С. С. Цифровая экономика как новая модель современного социально-экономического развития России / С. С. Носова, В. В. Рябцун, А. Н. Норкина // Экономика и предпринимательство. – М., 2018. – №3 (92). – С. 26–32.

80. Оздербиева, Ж. А. Влияние цифровой экономики на рынок труда / Ж. А. Оздербиева, О. И. Шершнева, А. Ю. Хирная // Экономика и предпринимательство. – М., 2018. – №6 (95). – С. 103–107.

81. Орехов, В. Д. Исследование новых тенденций и закономерностей воздействия цифровой экономики на производительность труда / В. Д. Орехов, М. С. Мельник, О. С. Причина // Проблемы экономики и юрид. практики. – М., 2018. – №2. – С. 20–25.

82. Основы цифровой экономики: учеб. пособие / Е. А. Бренделева, Ю. А. Гончаров, А. А. Коломейцева и др. – М.: Науч. б-ка, 2018. – 238 с.

83. Особенности регулирования трудовых отношений в условиях цифровой экономики: монография / И. Я. Белицкая, Д. Л. Кузнецов, Ю. П. Орловский, Д. В. Черняева; под ред. Ю. П. Орловского, Д. Л. Кузнецова; Нац. исслед. ун-т «Высш. школа экономики», Высш. школа

юриспруденции, при участии ПАО «ВымпелКом». – М.: Юрид. фирма Контракт, 2018. – 148 с.

84. Открытое правительство: сайт. – URL: http://open.gov.ru/events/5515775/ (дата обращения: 23.07.2020). – Текст: электронный.

85. Петрова, Е. В. Информационная среда и ее воздействие на человека: проблемы экологии человека в информационном обществе / Е. В. Петрова // Филос. науки. – М., 2017. – №5. – С .98–114.

86. Пещанская, И. В. Экономика информационного общества: взгляд двадцать лет спустя / И. В. Пещанская // Рос. экон. журн. – М., 2018. – №5. – С. 111–124.

87. Пименов, В. В. Экономическая и информационная безопасность в условиях цифровой трансформации: инструменты и механизмы по их нейтрализации / В. В. Пименов, П. К. Шафранский // Экон. безопасность и качество. – Саратов, 2018. – № 1 (30). – С. 25-30.

88. Пичков, О. Б. Перспективы и возможности цифровой экономики на современном этапе развития / О. Б. Пичков, А. А. Уланов // Страховое дело. – М., 2017. – №10. – С. 12–16.

89. Пичков, О. Б. Риски и несовершенства развития цифровой экономики на современном этапе / О. Б. Пичков, А. А. Уланов // Страховое дело. – М., 2017. – №11. – С. 3–8.

90. Попов, Е. В. Развитие человеческого капитала в условиях формирования цифровой экономики / Е. В. Попов, К. А. Семячков // Менеджмент в России и за рубежом. – 2018. – №3. – С. 91–99.

91. Производительность труда и факторы ее повышения в цифровой экономике: материалы Междунар. науч.-практ. конф., 15-16 февраля 2018 года / Воронеж. гос. ун-т, Экон. фак., Каф. общей экон. теории; под ред. И. Т. Корогодина, В. Г. Дайнеко. – Воронеж: Науч. книга, 2018. – 121 с.

92. Развитие цифровой экономики в России : Доклад Всемирного Банка. – URL: http://gosbook.ru/node/94904] (дата обращения: 17.04.2020). – Режим доступа: Электронный.

93. Развитие цифровой экономики в России. Программа до 2035 г. // Информационно-Аналитический портал Клуба субъектов инновационного и технологического развития России. – URL: http://innclub.info/wp-content/uploads/2017/05/strategy.pdf. (дата обращения: 21.08.2020). – Текст: электронный.

94. Регент, Т. М. Потенциалы человеческого капитала и цифровой экономики России / Т. М. Регент // Вестн. Рос. нового ун-та. Серия «Человек и о-во». – М., 2018. – Вып.1. – С. 97–102.

95. Репичев, А. И. Анализ и перспективы развития цифровой экономики в Российской Федерации / А. И. Репичев, Л. В. Тугачева, А. В. Павлова // Экономика и предпринимательство. – М., 2018. – №5 (94). – С. 137–143.

96. Рихтер, К. К. Цифровая экономика как инновация XXI века: вызовы и шансы для устойчивого развития / К. К. Рихтер, Н. В. Пахомова // Проблемы современной экономики. – СПб., 2018. – №2. – С. 22–31.

97. Рогалева, И. Ю. Особенности оформления трудовых отношений в цифровой экономике / И. Ю. Рогалева, Г. А. Рогалева // Вестн. Рос. экон. ун-та им. Г.В. Плеханова. – М., 2018. – №4 (100). – С. 184–189.

98. Росляков, А. В. Интернет вещей: учебное пособие / А. В. Росляков, С. В. Ваняшин, А. Ю. Гребешков. − Самара: ПГУТИ, 2015. − 200 с.

99. Россия онлайн? Догнать нельзя отстать. Отчет The Boston Consulting Group. – URL: http://imagesrc.bcg.com/Images/BCG-Russia-Online_tcm27-152058.pdf (дата обращения: 18.07.2020). – Текст: электронный.

100. Рунет. Экономика Рунета. Цифровая экономика: цифровой ресурс : сайт. – URL: http://rigf.ru/docs/plugotarenko.pdf (дата обращения: 18.07.2020). – Текст: электронный.

101. Савельева, Е. А. Сущность и функции регламентации труда при переходе к цифровой экономике // Экономика труда. – М., 2018. – Т.5, №1. – С. 1–12.

102. Савина, Т. Н. Цифровая экономика как новая парадигма развития: вызовы, возможности и перспективы // Финансы и кредит. – М., 2018. – Т.24, №3. – С. 579-590.

103. Сможет ли Россия стать центром инноваций: сайт. – URL: https://www.zelao.ru/13/29339-smojet-li-rossiya-stattsentrom-innovatsiy/ (дата обращения: 21.06.2020). – Текст: электронный.

104. Соловьев, А. И. Человек в цифровой экономике: аналоговый или дискретный? // Науч. тр. Вольного экон. о-ва России. – М., 2018. – Т. 210, №2. – С. 130–134.

105. Современное развитие России в условиях новой цифровой экономики: материалы II Междунар. науч.-практ. конф., 19-20 апреля 2018 года / Рос. экон. ун-т им. Г. В. Плеханова, Краснодар. фил. – Краснодар: Диапазон-В, 2018. – 479 с.

106. Стародубцева, Е. Б. Цифровая трансформация мировой экономики / Е. Б. Стародубцева, О. М. Маркова // Вестник АГТУ. Сер. Экономика. – 2018. – № 2. – С. 7–15.

107. Тоффлер, Э. Третья волна / Э. Тоффлер. – М.: АСТ, 2004. – 781 с.

108. Удалов, Д. В. Угрозы и вызовы цифровой экономики // Экон. безопасность и качество. – Саратов, 2018. – №1 (30). – С.12–18.

109. Урманцева, А. Цифровая экономика: как специалисты понимают этот термин / А. Урманцева // РИА Новости. – URL: https://ria.ru/science/20170616/1496663946.html (дата обращения: 10.07.2020). – Текст: электронный.

110. Усков, В. С. Формирование цифровой экономики в России в условиях четвертой промышленной революции и новой экономической реальности // Вестн. Владимир. гос. ун-та им. Александра Григорьевича и Николая Григорьевича Столетовых. Экон. науки. – Владимир, 2018. №3 (17). – С. 182–197.

111. Устюжанина, Е. В. Цифровая революция и фундаментальные изменения в экономических отношениях / Е. В. Устюжанина, А. В. Сигарев, Р. А. Шеин // Вестник Челябинского государственного университета. – 2017. – № 10 (406). – С. 15–25.

112. Федеральная служба государственной статистики: Росстат : официальный сайт. – Москва. – URL: http://www.gks.ru/ (дата обращения: 12.06.2020). – Текст: электронный.

113. Фешина, С. С. Цифровизация экономики: проблемы и последствия / С.С. Фешина, А. С. Славянов // Экономика и управление: проблемы, решения. – М., 2018. – №5, т.7. – С. 159–163.

114. Филин, С. А. Организационно-управленческие инновации как основа цифровой экономики / С. А. Филин, А. Ж. Якушев // Нац. интересы: приоритеты и безопасность. – М., 2018. – Т.14, Вып.7. – С. 1319–1332.

115. Халевинский, И. В. Цифровая экономика: как без нее сегодня // Междунар. жизнь. – М., 2018. – №8. – С. 105–114.

116. Хетагурова, Т. Г. Современные проблемы развития цифровой экономики / Т. Г. Хетагурова, И. Ю. Хетагурова // Экономика и предпринимательство. – М., 2017. – №9 (86), ч.2. – С. 763–767.

117. Цифровая экономика в социально-экономическом развитии России: сб. науч. тр. по итогам Всерос. науч.-практ. конф. молодых ученых С.- Петерб. гос. экон. ун-та / С.- Петерб. гос. экон. ун-т, Совет молодых ученых; под ред. Е. А. Горбашко. – СПб.: Изд-во С.- Петерб. гос. экон. ун-та, 2018. – 332 с.

118. Цифровая экономика: крат. стат. сб. / М-во связи и массовых коммуникаций Российской Федерации, Федер. служба гос. статистики, Высш. шк. экономики, Нац. исслед. ун-т. – Москва.: ВШЭ, 2018. – 95 с. – Текст : непосредственный.

119. Цифровая экономика: социально-экономические и управленческие концепции: монография / Л. И. Антонова, Д. И. Городецкий, А. Ф.

Золотарева и др.; науч. рук.: А. А. Степанов; Моск. гос. ин-т междунар. отношений, Рос. гос. социал. ун-т, Варненски свободен университет «Черноризец Храбър», Uczelnia techniczno-handlowa im. H. Chodkowskiej. – М. и др.: Виктория+, 2018. – 184 с.

120. Цифровая экономика и перспективы ее роста на 2018-2020 года / А. В. Захарян, Е. С. Померко, А. В. Негодова, М. А. Давыденко, Д. М. Ионова, С. А. Аристова // Экономика и предпринимательство. – М., 2018. – №5 (94). – С. 169–173.

121. Цифровая экономика: глобальные тренды и практика российского бизнеса / Отв. редактор Д. С. Медовников. – М.: НИУ ВШЭ, 2017. – 121 с.

122. Цифровая экономика: как специалисты понимают этот термин // РИА Новости-2017. – URL: https://ria.ru/science/20170616/1496663946.html (дата обращения: 11.08.2020). – Текст: электронный.

123. Цифровая Россия: новая реальность // Аналитический отчет экспертной группы Digital. ООО «Мак-Кинзи и Компания СиАйЭс», июнь 2017. – URL: www.mckinsey.ru (дата обращения: 07.05.2020). – Текст: электронный.

124. Цифровое будущее или экономика счастья? / А. В. Черновалов, З. Цекановский, З. Шиманьский, П. А. Черновалов. – М.: Дашков и К°, 2018. – 217 с.

125. Человек и общество в цифровой экономике: опыт, проблемы и направление развития: материалы Всерос. науч.-практ. конф., посвящ. 100-летию ФГБОУ ВО «Фин. ун-т при Правительстве Рос. Федерации» (18-19 апреля 2018 г.): сб. ст. / Новорос. фил. ФГБОУ ВО «Фин. ун-т при Правительстве Рос. Федерации»; отв. ред.: Е. Н. Сейфиева, М. В. Корниенко. – Краснодар: Издательский Дом – Юг, 2018. – 172 с.

126. Что важнее: реальная или цифровая экономика? // Планета коб. URL: https://www.planet-kob.ru/articles/6348 (дата обращения: 09.07.2020). – Текст: электронный.

127. Шибанова-Роенко, Е. А. Субъекты цифровизации: современное представление и оценка перспектив цифровой экономики (кризис-ориентированный обзорный анализ) // Друкеровский вестн. – Новочеркасск, 2018. – №3 (23). – С.43–59.

128. Ширинкина, Е. В. Драйверы развития рынка труда в цифровой экономике // Экономика и менеджмент систем управления. – Воронеж, 2018. – №3 (29). – С. 71–79.

129. Ширинкина, Е. В. Роль человеческого фактора в цифровом развитии российской экономики // Экономика и предпринимательство. – М., 2018. – №8 (97). – С. 182–185.

130. Щербакова, Л. Н. Противоречия становления информационной экономики: монография / Кемеров. гос. ун-т. – Кемерово: Кемеров. гос. ун-т, 2014. – 181 с.

131. Экономика знаний и роль человеческого капитала в ее формировании: монография / А. Л. Алавердян, И. Альнафра, Г. Г. Балабанова и др.; под ред. Е. Н. Чижовой. – Белгород: Белгород. гос. технол. ун-т им. В. Г. Шухова, 2018. – 281 с.

132. Экономика информационного общества: иллюзии и реальность // Ю. В. Грум-Гржимайло. Часть 1. Информационное общество. – 2010, вып. 2. – С. 12–20.

133. Эмирова, И. У. Виртуальные социально-трудовые отношения и их составляющие / И. У. Эмирова, Р. А. Тедеева, Т. В. Верховенко // Экономика и предпринимательство. – М., 2017. – №9 (86), ч.2. – С. 491–494.

134. Юдина Т. Н. Осмысление цифровой экономики / Т. Н. Юдина // Теоретическая экономика. – 2016. – №3. С. 12–16.

135. Юшкова, И. У. Особенности формирования и развития человеческого капитала в информационной экономике / И. У. Юшкова, И. В. Лукьянова // Инновационное развитие экономики: реалии и перспективы: материалы Междунар. науч.-практ. конф. проф.-пре-под. состава и аспирантов, 31 марта – 2 апреля 2015года. – Белгород, 2015. – Ч.1. – С. 393–399.

136. Neogronte, N.(1995)Being Digital Knopf (Paper edition 1996, Vintage Books)

137. Hearing The Digital Economy. – Paris: OECD, 2012. // OECD. – Mode of Access: http://www.oecd.org/daf/competition/ The-DigitalEconomy-2012.pdf. – Date of access: 02.07.2020.

138. Advancing Australia as a Digital Economy: An Update to the National Digital Economy Strategy. Canberra: Department of Broadband, Communications and the Digital Economy, 2013// DBCDE. – Mode of Access: http://apo.org.au/node/34523. – Date of access: 22.07.2020.

139. The Digital Economy. – London: British Computer Society, 2014 // BCS. – Mode of Access: http://policy.bcs.org/sites/ policy.bcs.org/files/digital%20economy%20Final%20version_0.pdf. – Date of access: 03.07.2020.

140. OECD Digital Economy Outlook 2015, OECD Publishing, Paris. 198

141. Challenges for Competition Policy in a Digitalised Economy. – Brussels: European Parliament, 2015 // Eoroparliament. – Mode of Access: http://www.europarl.europa.eu/Reg-Data/etudes/STUD/2015/542235/IPOL_STU%282015%29542235_EN.pdf. – Date of access: 20.06.2020.

142. Dahlman, C. Harnessing the Digital Economy for Developing Countries: Working Paper No. 334 / C. Dahlman, S. Mealy, M. Wermelinger. – Paris: OECD, 2016 // OECD. – Mode of Access: http://www.oecd-ilibrary.org/docserver/download/4adffb24-en.pdf. – Date of access: 02.07.2020.

143. Rouse, M. (2016) Digital Economy /M. Rouse // Newton: Techtarget. – Mode of Access: http://searchcio.techtarget.com/ definition/digital-economy. – Date of access: 15.05.2020.

144. World Investment Report 2017: Investment and the Digital Economy. – UNCTAD, 2017. – 238 p.

145. What is Digital Economy? – New York: Deloitte, 2017 // Deloitte. – Mode of Access: https://www2.deloitte.com/mt/en/pages/technology/articles/mt-what-is-digital-economy.html. – Date of access: 10.06.2020.

146. Digital Economy / Oxford: Oxford University Press, 2017 // Oxford Dictionary. – Mode of Access: https://en.oxfordd ictionaries.com/definition/digital_economy. – Date of access: 11.06.2020.

147. Singh S., Jeong Y., Park J. H. A survey on cloud computing security: Issues, threats, and solutions // Journal of Network and Computer Applications 75 (2016) − P. 200-222.

148. The Intel IoT Platform: Architecture Specification White Paper. – URL: https://www.intel.sg/content/www/xa/en/internet-of-things/white-papers/iot-platform-reference-architecture-paper.html (дата обращения: 10.06.2020). – Текст: электронный.

149. Microsoft Azure IoT Reference Architecture. – URL:https://aka.ms/iotrefarchitecture (дата обращения: 07.06.2020). – Текст: электронный.

150. Industrial Internet Reference Architecture // Industrial Internet Consortium (IIRA). – URL: https://iiconsortium.org (дата обращения: 11.06.2020). – Текст: электронный.

151. Ammar M., Russello G., Crispo B. Internet of Things: A survey on the security of IoT frameworks // Journal of Information Security and Applications 38 (2018) – P.8-27. - URL: https://doi.org/10.1016/j.jisa.2017.11.002 (дата обращения: 11.06.2020). – Текст: электронный.

*Научное издание*

**Джабраилова Лаура Хамзатовна**

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК ПРИОРИТЕТНОЕ НАПРАВЛЕНИЕ РАЗВИТИЯ ЦИФРОВОЙ ЭКОНОМИКИ**

***Монография***

Подготовка оригинал-макета *Керимова Н.А.*
Дизайн обложки *Эскаева Г.А.*

---

Подписано в печать 18.12.2020 г. Формат 60x84 1/16.
Гарнитура «Таймс». Бумага офсетная. Печать ризографная.
Усл. п. л. 6,7. Уч.- изд. л. 6. Тираж 1000 экз. Заказ №20-12-612.

Отпечатано в типографии АЛЕФ
367002, РД, г. Махачкала, ул. С.Стальского 50, 3 этаж
Тел.: +7 (8722) 935-690, 599-690, +7 (988) 2000-164
www.alefgraf.ru, e-mail: alefgraf@mail.ru