Учреждение образования
«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ
ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

В. Б. Криштаносов

ЦИФРОВИЗАЦИЯ ЭКОНОМИКИ РЕСПУБЛИКИ БЕЛАРУСЬ И НАЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ: СОВРЕМЕННЫЕ КОНЦЕПТУАЛЬНО-АНАЛИТИЧЕСКИЕ ПОДХОДЫ

Монография

В 2-х томах

Том 1

Минск 2023

УДК 338.2-027.45(476)
ББК 65.20
К82

Рассмотрена и рекомендована к изданию редакционно-издательским советом учреждения образования «Белорусского государственный технологический университет».

Р е ц е н з е н т ы :
директор Белорусского института стратегических исследований доктор юридических наук *О. С. Макаров*;
проректор по научной работе
УО «Белорусский государственный экономический университет»
доктор экономических наук, профессор *А. А. Быков*

Криштаносов, В. Б.

К82 Цифровизация экономики Республики Беларусь и национальная безопасность: современные концептуально-аналитические подходы : монография : в 2 т. / В. Б. Криштаносов. – Минск : БГТУ, 2023. – Т. 1. – 347 с.

ISBN 978-985-897-063-5.

Монография раскрывает проблематику разработки и внедрения эффективных механизмов прогнозирования и регулирования рисков цифровизации, связанных с нарастающими технологическими изменениями, в разной степени меняющими структуру экономики и формирующими как новые точки роста, так и возможные угрозы стабильного функционирования систем на макро- и микроуровнях.

Материалы монографии могут представлять практический интерес для органов государственного управления в рамках компетенции, при разработке проектов законодательства по регулированию национальной экономики в контексте национальной экономической безопасности.

УДК 338.2-027.45(476)
ББК 65.20

ISBN 978-985-897-063-5 (Т. 1)
ISBN 978-985-897-062-8

ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ

В настоящее время развитие множества сфер общественной жизни определяется стремительной динамикой внедрения цифровых технологий, которые становятся определяющим фактором конкурентоспособности как отдельных предприятий, так и государств в целом.

Нарастающие технологические изменения, в разной степени меняющие структуру экономики развитых и развивающихся государств, формируют новые (либо потенциальные) точки роста. Вместе с тем активная цифровизация генерирует новые риски и угрозы, связанные со стабильностью функционирования финансовых и платежных систем. Кроме того, органы государственного управления сталкиваются с острой необходимостью не столько адаптации сложившихся практик регулирования, сколько формирования нового инструментария, позволяющего не только контролировать (регулировать) происходящие изменения, но и эффективно использовать те преимущества, которые они открывают для развития национальной цифровой экономики в современных условиях глобализации и конкуренции.

С учетом изложенного в монографии представлена авторская модель институциональной регуляторной экосистемы цифровой экономики, выделены осорбенности ее реализации на национальном (США, КНР, Российская Федерация) и наднациональном (ЕС, ЕАЭС) уровнях. При этом проведен сравнительный анализ данных экосистем в динамике.

Кроме того, в представленном исследовании выделены ключевые блоки рисков имплементации технологических решений IoT, Cloud, AI, BDA, Блокчейн, для основных концептов Industry 4.0, Agriculture 4.0, Smart Grid, Smart Supply Chain, E-Commerce и Smart City, отмечены общие и специфические группы рисков и угроз, включая формирование оцифрованных сред в форме двух взаимосвязанных сетей: информационной и производственной.

Республика Беларусь ввиду малого открытого типа национальной экономики находится под влиянием мировых тенденций цифровизации, которые формируют предпосылки для повышения

конкурентоспособности как продукции, так и экономической модели в целом. Вместе с тем наша страна сталкивается и с растущей проблематикой обеспечения экономической безопасности, связанной с внедрением новых цифровых технологий в ключевые сферы жизнедеятельности государства. В представленной монографии приведен анализ данных рисков и угроз с учетом современных подходов к оценке цифровых рисков, анализа угроз на макроэкономическом уровне и в секторальном разрезе и ее методик, включая E-Government, CBDC, FinTech, проблемы сокращающейся занятости, цифрового разрыва и пр.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И (ИЛИ) УСЛОВНЫХ ОБОЗНАЧЕНИЙ

АЗС – атака захвата сеанса
АИСС – атака с использованием методов социальной инженерии
АИЭЗ – атака на инфраструктуру электронного здравоохранения
АКИ – атака на критическую инфраструктуру
АПР – атака на промышленных роботов
АРИИ – атака раскрытия идентификационной информации
АСЕАН – Ассоциация государств Юго-Восточной Азии
АЦП – атака цепочки поставок
АЧ – атака червоточины
АЧД – атака «черная дыра»
БИСРС – Белорусская интегрированпная сервисно-расчетная система
БОИНСБ – Бюро общественной информации и надзора за сетевой безопасностью КНР
ВБК/ВКК – взломы биржевых и криптовалютных кошельков
ВЕЭС – Высший Евразийский экономический совет
ВП – вредоносные программы
ГосСОПКА – система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ
Госстандарт – Государственный комитет по стандартизации Республики Беларусь
ДТ – двойная трата
ЕРИП – Небанковская кредитно-финансовая организация «Единое расчетное информационное пространство»
ЕЭК – Евразийская экономическая комиссия
ИКТ – информационно-телекоммуникационные технологии
ИПИД – использование поддельных (краденых) идентификационных данных
ИТ – информационные технологии
КЕЭК – Коллегия Евразийской экономической комиссии

ККиС – коммерческий кибершпионаж и саботаж
Кр – криптоджекинг
КЦД – кража цифровых (личных) данных
М – использование сервисов (миксеров)
МА – маскарадная атака
Майнинг – процесс сбора и обработки информации обо всех операциях, в данный момент происходящие в сети Блокчейн, который вознаграждается
МАР – атака маршрутизации
Минсвязи – Министерство связи и коммуникаций Республики Беларусь
Минцифры – Министерство цифрового развития, связи и массовых коммуникаций Российской Фдерации
МО – мошеннические операции
MOSIM – мошенничество с обходом или мошенничество с SIM
МСИ – межбанковская система идентификации Республики Беларусь
МСП – малое и среднее предпринимательство
МНК – многонациональная корпорация
МПИ – Министерство промышленности и информатизации КНР
МС – Межправительственный совет ЕАЭС
МСП – малое и среднее предпринимательство
МЦ – Министерство цифровизации
МЦР – Министерство цифрового развития, связи и массовых коммуникаций РФ
Мэйнфрейм-компьютер – большой высокопроизводительный сервер с большими вычислительными ресурсами
МЭР – Министерство экономического развития РФ
Нацбанк – Национальный банк Республики Беларусь
НКЦКИ – Национальный координационный центр по компьютерным инцидентам РФ
ОАЦ – Объединенный аналитический центр при Президенте Республики Беларусь
ОЭСР – Организация экономического сотрудничества и развития
ПАТ – прослушивание и анализ трафика
ПВТ – Парк высоких технологий

ПBSCADA – программы взлома систем управления производством
ПИА – поддельная информационная атака
ПО – программное обеспечение
ПОД-ФТ – подход FATF к «противодействию отмыванию денег и финансированию терроризма»
ПУОИ – потеря управления при использовании облачной инфраструктуры
РВК – Российская венчурная компания
«Регуляторная песочница» – кластер, на который не распространяются отдельные действующие законодательные, организационные, административные, технические нормы и ограничения
СЕЭС – Совет Евразийской экономической комиссии
Смарт-контракт – гарантированное программным обеспечением выполнение простых односложных условий в Блокчейн
ТНК – транснациональная корпорация
УАИ – узловая атака имитации
УАСУ – удаленная атака на системы управления трафиком
ЦБ – Центральный банк РФ
ЦИСЗ – централизованная информационная система здравоохранения Республики Беларусь
ЦУР – Цели устойчивого развития ООН
ЭУПО – эксплуатация уязвимостей ПО
Эфир – единица криптовалюты Блокчейн платформы Ethereum
ЮНКТАД – Конференция ООН по торговле и развитию
Additive Manufacturing, 3D – концепция «аддитивного производства»
AFI – Альянс за финансовую доступность
AI – искусственный интеллект
AII – Альянс промышленного Интернета (КНР)
AIS – информационная услуга счета Директивы ЕС PSD2
AITS – система идентификации, регистрации, прослеживаемости животных и продукции животного происхождения
AMON – Оперативная сеть по борьбе с отмыванием денег

API – программный интерфейс приложения
APT – целевые кибератаки
Aquaponics – концепция «аквапоника»
ARDL – модель авторегрессионного распределенного запаздывания
ASIC – Австралийская комиссия по ценным бумагам и инвестициям
AT – алгоритмическая торговля
A4.0, Agriculture 4.0 – концепция «сельского хозяйства 4.0»
BaaP – концепция «банковское дело – как платформа»
BaaS – концепция «банковское дело – как услуга»
BDA, Big Data Analytics – аналитика больших данных
BIM – системы информационного моделирования в области промышленного и гражданского строительства
Bioeconomy – концепция «биологической экономики», «биоэкономики» или «биотехнологии»
BIS – Банк международных расчетов
BPM – процессное управление организацией
BU – базовая единица системы цифровой экономики
B2B – экономическое взаимодействие на уровне коммерческих организаций
B2C – экономическое взаимодействие на уровне бизнес-организация – потребитель
CaaS – «киберпреступление как услуга»
CAD, CAE – системы цифрового проектирования и моделирования
CAPP – системы планирования производства
CAC – Администрация киберпространства КНР
CBDC – цифровые валюты центральных банков
CBOE – Чикагская биржа опционов
CBSC – Комиссия по банковскому надзору КНР
CEIB – Центральное бюро экономической разведки Индии
CEN – Европейский комитет по стандартизации
CenCIP – Шведский центр исследований защиты критической инфраструктуры
CFPB – Бюро финансовой защиты потребителей США

CFSP – Общая внешняя политика и политика безопасности ЕС
CFTC – Комиссия по торговле товарными фьючерсами США
CGAP – Консультативная группа по оказанию помощи бедным
CIA – Метод оценки рисков «Конфиденциальность, целостность и доступность»
CIPAC – Консультативный совет по критическому инфраструктурному партнерству США
Circular Agriculture – концепция «циркулярного сельского хозяйства»
CISA – Агентство по кибербезопасности и безопасности инфраструктуры США
CISC – Комиссия по надзору за страхованием КНР
CIWIN – Европейская сеть предупреждений о критической инфраструктуре
Cloud Computing – концепция «облачных вычислений»
Cloud Manufacturing – концепция «облачного производства»
CME – Чикагская товарная биржа
Cobots – коллаборативные роботы
CPS – киберфизические системы
CPMC – концепция «облачного киберфизического производства»
Crowdfunding – краудфандинг
CSDP – Общая политика безопасности и обороны ЕС
CSF – «Структура кибербезопасности» NIST
CSIRT – группа реагирования на инциденты компьютерной безопасности
CSSC – Комиссия по надзору за ценными бумагами КНР
CVSS – Общая систему оценки уязвимостей NIAC
CWA – Рабочее соглашение по управлению возникающими рисками, связанными с технологией CEN
C_TEC – Центр по взаимодействию с технологиями Торговой палаты США
C2C – экономическое взаимодействие на уровне «потребитель – потребитель»
DAMP – платформы цифрового управления активами

DAO – децентрализованная автономная организация, функционирующая исключительно по правилам, зафиксированным в смарт-контрактах на Блокчейн

DApp – веб-приложения, которые взаимодействуют с экосистемами Блокчейн

DarkMarket – платформа по реализации запрещенных в свободном обороте товаров и услуг

DDoS – кибератака «распределенный отказ в обслуживании»

DeFi – децентрализованные финансы

DEI – Инициатива ЕС по цифровизации европейской промышленности

DEMA – Датское агентство по управлению чрезвычайными ситуациями

DHS – Министерство национальной безопасности США

Digital Agriculture – концепция «цифрового земледелия»

Digital Twins – концепция «цифровых близнецов»

Distributed Manufacturing – концепция «распределенного производства»

DLT – технология распределенного реестра

DoS – кибератака «отказ в обслуживании»

DOT – Министерство транспорта США

EBA – Европейское банковское управление

ECB – Европейский центральный банк

ECDS – Стратегия внедрения облачных технологий ЕС

Eclipse – атака, предполагающая изоляцию конкретного узла одноранговой сети

ECSO – Европейская организация кибербезопасности

EC3 – Европейский центр киберпреступности при Европоле

Edge Computing – концепция «пограничных вычислений»

EDPS – Европейский надзорный орган по защите данных

eGMM – модели зрелости E-Government

EMIR – Регламент инфраструктуры рынка ЕС

ENISA – Европейское агентство по информационной безопасности сетей

EPCIP – Европейская программа защиты критической инфраструктуры

EPI – Европейская платежная инициатива
ERM – риски управления на уровне предприятия
ERP – цифровая система планирования ресурсов предприятия
ESMA – Европейское управление по ценным бумагам и рынкам
ETF – биржевые фонды
Ethereum – глобальная платформа для создания смарт-контрактов
ETSI – Европейский институт телекоммуникационных стандартов
EU4Digital – Инициатива Европейского Союза по цифровому развитию Восточного партнерства
E-Commerce – электронная коммерция
E-Government – концепция «цифровое правительство»
FATF – Группа разработки финансовых мер борьбы с отмыванием денег
FCA – Управление финансового поведения Великобритании
FDIC – Федеральная корпорация страхования депозитов США
FinCEN – Агентство по борьбе с финансовыми преступлениями США
FINRA – Служба регулирования отрасли финансовых услуг США
FinTech – финансовые технологии либо компании, оказывающие технологичные (цифровые) финансовые услуги
FIPS – Федеральные стандарты информации США
FISMA – Федеральный закон об управлении информационной безопасностью США
Fog Computing – концепция «туманных вычислений»
FSB – Совет по финансовой стабильности
FSC – Комиссия по финансовым услугам Кореи
FSOC – Совет по надзору за финансовой стабильностью США
FTC – Федеральная торговая комиссия США
GDPR – Общее положение о защите данных ЕС
GFIN – Глобальная сеть финансовых инноваций
GLN – проект Глобальная сеть маяков

GPFI – Глобальное партнерство по финансовой доступности
GPON – технология пассивных оптических сетей
GPS атака – атака, направленная на взлом управления положением транспортных средств
GSA – Управление общих служб США
G20 – Большая двадцатка (Группа двадцати)
IFR – Международная федерация робототехники
HFT – высокочастотная алгоритмическая торговля
HLF – протокол на платформе IBM Watson IoT
HMRC – налоговая служба Великобритании
IaaS – облачный сервис «инфраструктура как услуга»
ICO – первичное размещение монет (токенов)
ICS – промышленные системы управления
IDC – Международная корпорация данных
IEA – Международное энергетическое агентство
IEC – Международная электротехническая комиссия
IEEE – Институт инженеров электротехники и электроники
IEO – первоначальное биржевое предложение
IETF – Инженерная рабочая группа по Интернету
IFISA – Инновационный финансовый индивидуальный сберегательный счет Великобритании
IIC – Промышленный Интернет-консорциум
IIoT – промышленный Интернет вещей
Insurech – технологический концепт «цифровизации страховой деятельности»
INTCEN – Разведывательный и ситуационный центр ЕС
IOSCO – Международная организация комиссий по ценным бумагам
IoT – концепция «Интернета вещей»
IRGC – Международный совет по управлению рисками
IRS – Служба внутренних доходов США
ISMS – система управления информационной безопасностью
ISO – Международная организация по стандартизации
ITS, Intellectual Transport System – концепция «интеллектуальной транспортной системы»

ITU – Международный союз электросвязи
I4.0, Industry 4.0 – технологический концепт «промышленность 4.0»
J-CAT – Совместная целевая группа ЕС по борьбе с киберпреступностью
KM – управление знаниями и навыками на различных уровнях
KYC – подход FATF «Знай своего клиента»
KYCC подход FATF «Знай клиентов своих клиентов»
KYD – подход FATF «Знай свои данные»
MAD – Директива ЕС о злоупотреблении рынком
MATH – модель принятия и технологий в домашних хозяйствах
MC – вредоносный контроль над системой
MES – цифровая система управления производственными процессами
Man-in the-Middle – атака через посредника
MIF – Руководство ЕС по комиссиям за обмен по платежным картам
MiFID – Директива ЕС о рынках финансовых инструментов
MiFIR – Регламент ЕС о рынках в финансовых инструментах
MIS – информационная система управления
ML, Machine Learning – концепция «машинное обучение»
MNO – операторы мобильных сетей
MSB – Шведское агентство по чрезвычайным ситуациям в гражданском секторе
M2M – цифровое взаимодействие между удаленными устройствами
NCC – Национальный центр кибербезопасности КНР
NHS – Национальная служба здравоохранения Великобритании
NHTSA – Национальное управление безопасности дорожного движения США
NIAC – Национальный инфраструктурный консультативный совет США

NIHS – Национальный институт безопасности городов США
NIS – национальная инновационная система
NIS2 – Директива о безопасности сетевых и информационных систем ЕС
NIST – Национальный институт стандартов и технологий США
NRMC – Национальный центр управления рисками США
OCC – Управление валютного контролера США
OCTAVE – метод оценки рисков в отношении критически важных для эксплуатации активов и уязвимостей
OFAC – Управление по контролю иностранных активов США
OMFIF – Официальный форум валютно-финансовых институтов
OTR – соотношение заказов и продаж
PA, Precision Agriculture – концепция «точное земледелие»
PaaS – облачный сервис «платформа как услуга»
PBC – Народный банк Китая
PBFT – задача Византийских генералов в Блокчейн
PDM – системы управления инженерными данными
Phishing, ФА – фишинговая атака
PFMI – Принципы инфраструктуры финансового рынка BIS
PIS – служба инициирования платежей
PLC, CALS – системы управления жизненным циклом промышленного продукта
PoET – доказательство прошедшего времени в Блокчейн
Polkadot – криптовалюта на основе Блокчейн Polkadot
PoS – доказательство доли владения в Блокчейн
POS – точка продажи
PoW – доказательство выполнения работы в Блокчейн
Prosumer – индивидуум, который выступает одновременно и как производитель, и как потребитель
PSD2 – Вторая Директива ЕС о платежных услугах
PwC – PriceWaterhouseCoopers
P2B – экономическое взаимодействие на уровне «физическое лицо – юридическое лицо»

P2P – экономическое взаимодействие на уровне физических лиц (одноранговое взаимодействие)
RaaS – «программа-вымогатель как услуга»
RBV – модель управления на основе ресурсов
RegTech – технологический концепт «цифровизации банковской отчетной деятельности»
REMIT – Положение ЕС о целостности и прозрачности оптовых энергетических рынков
Ripple – криптовалюта на основе протокола Блокчейн без использования майнинга
ROI – рентабельность инвестиций
RTGS – система валовых расчетов в реальном времени
R3 – протокол для работы в регулируемых средах с ограниченным числом известных участников
SaaS – облачный сервис «программное обеспечение как услуга»
SAIC – Государственная администрация для промышленности и торговли КНР
SAG – стратегическая консультативная группа по разработке Industry 4.0/Smart Manufacturing
SAMR – Управление по регулированию рынка КНР
SC – атака сканирования цифровых потоков
SCADA, CAM – системы автоматизации цеховых процессов
SCM – системы управления цепочками поставок
SEC – Комиссия по ценным бумагам и биржам США
SEPA – Единая европейская платежная зона
SFTR – Регулирование операций с финансированием ценных бумаг ЕС
Smart Building – технологический концепт «умное здание»
Smart City – технологический концепт «умный город»
Smart Factory – технологический концепт «умное производство»
Smart Farming – технологический концепт «умное земледелие»
Smart Government – технологический концепт «умное правительство»
Smart Grid – технологический концепт «умная электрическая сеть»
Smart Supply Chain – технологический концепт «умная логистика поставок»
SRA – Общество по анализу рисков

SSM, CRM – системы продажи и управления сервисом
STRIDE – метод оценки рисков Microsoft
SWOT – анализ сильных и слабых сторон
Sybil – атака узла IoT
TAM – модель принятия технологий
TCP/IP – сетевая модель передачи данных, представленных в цифровом виде
TDS – система доставки технологий
Telemedicine – технологический концепт удаленного мониторинга за состоянием здоровья пациентов, диагностика заболеваний
Tether – наиболее популярный в настоящее время стейблкоин
TIS – система технологических инноваций
TOE – технологии, организация и среда
TPB – теория планового поведения
TQM – модули общего управления качеством
TRA – теория рационального действия
TTF – модель соответствия задач технологиям
UNISDR – Международная стратегия ООН по уменьшению опасности стихийных бедствий
UTAUT – единая теория принятия и использования технологии
VANET – концепция «специальных автомобильных сетей»
Vertical farming – технологическая концепция «вертикального земледелия»
V2I – протокол связи «транспортное средство – инфраструктура»
V2N – протокол связи «транспортное средство – сеть»
V2V – протокол связи «транспортное средство – транспортное средство»
V2X – протокол связи «транспортное средство – любые объекты»
Wearables – технологическая концепция «умная одежда»
WEF – Всемирный экономический форум
WIPO – Глобальный индекс инновационности
W3C – Консорциум Всемирной паути́ны
3GPP – проект «Партнерство третьего поколения»
5G – пятое поколение мобильной связи, телекоммуникационный стандарт связи

Глава 1

ЭВОЛЮЦИОННО-ИНСТИТУЦИОНАЛЬНАЯ МЕТОДОЛОГИЯ ИССЛЕДОВАНИЯ ЭКОНОМИЧЕСКОГО РАЗВИТИЯ: ЦИФРОВЫЕ ИННОВАЦИИ, СМЕНА ТЕХНИКО-ЭКОНОМИЧЕСКОЙ ПАРАДИГМЫ, «НОВАЯ ЭКОНОМИКА»

Формирование современной концепции цифровой экономики базируется на ряде теоретических подходов, отражающих изменение ее состояния, качественных характеристик, тенденций и динамики развития. Внедрение цифровых инноваций приводит к развитию новых отраслей, сегментов и экономических систем, что актуализирует теоретические подходы, техно-экономические парадигмы, которые опираются, в том числе, на более ранние исследования и концепции, сформированные в мировой экономической науке.

1.1. Подрывные инновации в смене технико-экономической парадигмы: теоретико-концептуальные подходы

Исходной концепцией, предопределяющей изменение состояния экономических систем, является развитие. Понятие «развитие», с точки зрения классической философии предполагает необратимое, направленное, закономерное изменение материальных и идеальных объектов. В результате «развития» возникает новое качественное состояние объекта, которое выступает как изменение его состава или структуры, – возникновение, трансформация или исчезновение его элементов и связей [1]. С точки зрения экономики термин «развитие» может применяться для обозначения длительного процесса, затрагивающего совокупность экономических и социальных структур [2]. Экономическое развитие также трактуется как структурная перестройка экономики в соответствии с потребностями технологического и социального прогресса [3].

Концепция экономического развития как волнообразного процесса, который обусловлен технологическими инновациями, предложена в 1922 году Н. Д. Кондратьевым, который, в результате исследования уровня цен, процентных ставок, внешней торговли, заработной платы, банковских депозитов и других данных, отражающих изменения спроса и предложения в экономиках США, Германии, Великобритании и Франции, подтвердил существование длительных деловых циклов. Он доказал систематический переход капиталистических экономик от депрессии к устойчивому экономическому восстановлению [4]. Новые технологии и инновации способствуют переходу экономики в период спада в стадию развития.

Таким образом, идея технико-экономических парадигм стала одним из способов концептуализации взаимодействия между технологическими изменениями и изменениями в экономических условиях, а также процессом подрывных инноваций.

Технико-экономическая парадигма воплощает в себе относительно стабильный кластер основных технологий, вокруг которого происходят инновации и экономическая деятельность [5]. Технологии, оказывающие сильное влияние на экономику и общество, классифицируются в качестве основных с точки зрения потенциала для обобщения и проникновения в широкий спектр продуктов и процессов во все сектора экономической и зачастую человеческой деятельности.

В рамках парадигмы инновации происходят, когда основные технологии становятся все более распространенными и влияют на все более широкие сферы производства и распределения. При серьезном технологическом прогрессе, нарушающем существующие базовые технологии и способы экономической работы в большинстве отраслей, возникает новая технико-экономическая парадигма [6]. Смещение основных технологий старой парадигмы создает новую волну изобретений и инноваций и больше не связано с предыдущими основными технологиями парадигмы. Появление новой базовой технологии требует и создает возможность для целого нового набора небольших и дополнительных инноваций, которые позволяют широко использовать новые базовые технологии. Таким образом, когда происходит сдвиг в технико-экономической парадигме, мы имеем не только «эффект замещения», но и расширение креативной границы, которая обеспечивает появление новых технологий и, в конце концов, позволяет перейти к следующей парадигме.

Кроме того, помимо технологических и чисто экономических факторов, социальные и институциональные рамки, которые соответствуют определенной технико-экономической парадигме, могут не подходить для новой. Действительно, процесс возникновения новой технико-экономической парадигмы является результатом взаимодействия технологической, экономической, институциональной и социальной сфер. Наличие только новой технологии может не иметь никакого эффекта, если ряд изменений в других измерениях не сопровождает технологическую новизну. Определенный набор институтов и их социальных функций может обеспечить достаточный контекст для инноваций в рамках определенной парадигмы; иными словами, необязательно создавать институты и социальные правила в том же темпе, в котором развиваются технологические инновации. Но когда происходит смена технико-экономической парадигмы, может потребоваться новая институциональная структура для поддержания последующего развития.

Одним из основоположников теории технико-экономических парадигм является Дж. Шумпетер [7], который определял «инновации» как «новые комбинации» новых или существующих знаний, ресурсов, оборудования и других, отмечая новые изменения, происходящие в развитии продуктов, производственных процессов, рынков, ресурсов, материалов и организационных форм [8]. Он утверждал, что именно ожидание прибыли и временной монопольной позиции мотивируют «предпринимателя» к инновациям. Этот процесс Шумпетер назвал «творческим разрушением» [9]. Он подчеркивал значимость инноваций как переднего края экономического прогресса, который способствует экономическому процветанию. В своей работе [10] Шумпетер усовершенствовал более раннюю упрощенную версию предпринимателя на идеальном рынке, состоящем из множества конкурирующих фирм, которые разрушают любое постоянное рыночное преимущество, признав возможность некоторых крупных корпораций поддерживать рыночные преимущества путем институционализации усилий по внедрению инноваций посредством создания крупных исследовательских центров.

Переосмысление фундаментальных идей Шумпетера об инновациях как процессе неравновесия в более широком контексте технико-экономической парадигмы осуществлено, прежде всего, К. Фрименом и его соавторами. Этот подход, часто называемый «неошумпетерианским», сформулирован Фрименом, Кларком и Соетом [11], которые

обобщили концепцию инноваций Шумпетера на национальном уровне. Вместе с тем, если Шумпетер концептуализировал качественную трансформацию экономики, Фримен и Перес [12, 13] утверждали, что процесс экономического развития является радикальным и требует новой технико-экономической парадигмы. Согласно их исследованиям, технико-экономическая парадигма представляет собой совокупность взаимосвязанных технических, организационных и управленческих инноваций, которая затрагивает всю экономику.

Следует отметить, что теория Шумпетера об экономическом развитии заложила основу для дальнейшей разработки новой парадигмы [14, 15, 16]. Цикл развития промышленности представлен революционными сдвигами, в которых одна парадигма вытесняет другую, что приводит к скачкам экономического роста [9, 17].

Фримен и Соет предложили следующую периодизацию внедения технологий и их влияние на эволюцию развития экономики и производства в рамках парадигмы Кондратьева – Шумпетера о «последовательных промышленных революциях» [5, 18] (табл. 1.1).

Таблица 1.1

Этапы последовательных промышленных революций [18]

Этап эволюции	Отдельные характеристики технологических и организационных инноваций	Период, годы
Легкая механизация	Частные предприниматели и малые компании, локальный капитал, частное богатство	1770–1840
Паровая сила и железные дороги	Конкуренция малых фирм, появление беспрецедентно крупных компаний, корпорации с ограниченной ответственностью, акционерный капитал	1830–1890
Электрификация и тяжелая промышленность	Гигантские компании, картели, трасты, государственное регулирование, усиление антимонопольного регулирования, профессиональные команды управления	1880–1940
«Фордизм» и конвейерное производство	Олигопольная конкуренция, появление мультинациональных корпораций, рост ПИИ, вертикальная интеграция стилей и подходов технократического управления	1930–1980
Информатизация и компьютеризация	Компьютерные сети больших и малых компаний, волна предпринимательства на основе новых технологий, сильные региональные кластеры инновационных и предпринимательских компаний	1970-е – по н. в.

В развитие данной технико-экономической парадигмы Фримен и Локка детализировали периодизацию, расширив временные интервалы внедрения и характеристики экономических нововведений [19] (табл. 1.2).

Таблица 1.2

Этапы последовательных промышленных революций [20]

Этап эволюции	Отдельные характеристики технологических и организационных инноваций	Начало и конец периода, годы
Механизация промышленности за счет использования энергии воды	Заводские системы, предприниматели, партнерство	1780–1815/ 1815–1848
Паровая механизация промышленности и транспорта	Акционерные компании, субконтракты для ответственных ремесленников	1848–1873/ 1873–1895
Электрификация промышленности, транспорта и жилья	Специализированные профессиональные системы управления, гигантские компании, «тейлоризм»	1895–1918/ 1918–1940
Моторизация транспорта, гражданской и военной экономики	Конвейерное производство, массовое потребление, «Фордизм», новые иерархии	1941–1973/ 1973
Компьютеризация экономики	Внутренние, локальные и глобальные сети	1970-е – по н. в.

Китайские исследователи [21] предложили периодизацию промышленных революций, добавив современные этапы «эры сетей» и «киберфизических систем» (табл. 1.3).

Таблица 1.3

Этапы технологических инноваций

Период, годы	Название этапа инноваций
1800–1900	Эра механизации
1900–1950	Эра электрификации
1950–1980	Эра информатизации
1980–2010	Эра сетей
2010–по н. в.	Эра киберфизических систем

Рамирез-Пена, Санчес Сотано, Перес-Фернандес, Абад, Батиста [22] на основе концепции «Промышленной революции 4.0»,

предложенной Министерством промышленности и энергетики ФРГ [23], выделяют четыре революционных этапа развития промышленности и производства (табл. 1.4).

Таблица 1.4

Четыре революционных этапа развития промышленности

Этап	Описание и характеристики этапа
1-я промышленная революция сер. XIX – конец XIX века	Кустарный характер производства. Для того, чтобы генерировать большую экономическую прибыль, требовалось увеличивать производительность производства
2-я промышленная революция конец XIX – сер. XX века	Промышленное производство и электрическая энергия выступали главными драйверами развития. В дополнение к экономической и энергетической эффективности растет важность сохранения окружающей среды
3-я промышленная революция сер. XX – конец XX века	Использование электроники и вычислительной техники. Функциональность стала новым параметром модели эффективности бизнеса
4-я промышленная революция с 2015 года – по н. в.	С 2015 года появляются новые передовые производственные модели, новые технологии, позволяющие оцифровывать процессы, продукты, услуги и бизнес-модели

Веблен является одним из первых экономистов, который системным образом проанализировал взаимодействие институтов и преобразующую силу технологических инноваций, их влияние на институциональную структуру [24]. Технологическое развитие способствует росту человеческих знаний, что, в свою очередь, оказывает кумулятивное влияние на социальные установки, индивидуальное и коллективное поведение, технологические инструменты и социальные институты. Посредством концепции «совокупной причинности» (cumulative causation) Веблен объясняет динамику процесса, который приводит к прогрессивным институциональным изменениям. Так, технологические инновации изменяют объективные обстоятельства сообщества; новый набор обстоятельств изменяет привычки мышления и поведения; эти новые привычки мышления и поведения проецируются в другие области опыта сообщества, что порождает дальнейшие инновации в области искусства и науки, которые, в свою очередь, приводят к новым технологическим инновациям [25].

Анализ подходов к пониманию природы, условий возникновения и влияния инноваций на экономические, социальные и технологические изменения позволил выделить ряд ключевых современных парадигм инноваций, включая пользовательские, открытые, подрывные, основанные на дизайне, социальные, государственные, ответственные, основанные на знаниях, бережливое производство, инновации конвергенции, Jugaad инновации, местные, полные, вторичные.

В отличие от инновационных парадигм, разработанных в Соединенных Штатах Америки, которые ориентированы в первую очередь на рынок и коммерциализацию, парадигмы, разработанные в Европе, сфокусированы больше на инновационной миссии, а не на экономических атрибутах, и уделяют внимание более широкой макроэкономической ценности на социальном уровне [26].

Ряд американских ученых провели исследования с точки зрения экономики технологических изменений [27], изучая связь между промышленными исследованиями и технологическими инновациями [28], а также стимулирующее влияние технологических инноваций на экономический рост и социальное конкурентное преимущество [29].

Тушман и Андерсон [30] также описывают паттерны технологических изменений как кумулятивный процесс до стадии, когда появляются разрывающие инновации. Это вызывает технологические сдвиги – либо повышающие компетенцию, либо разрушающие компетенцию. Разрывы, способствующие повышению компетентности, представляют собой улучшения на порядок, основанные на накопленном опыте использования более ранних выпусков технологий, в отличие от разрывов, разрушающих компетенции, которые требуют овладения новыми технологиями, навыками, способностями и знаниями как в разработке, так и в производстве продукта [31].

Теория распространения инноваций тесно связана с инновационным процессом. Уттербек и Абернати [32] формулируют инновационный процесс как S-шаблон. Вернон предложил концепцию жизненного цикла продукта (Product Life Cycle PLC) в рамках классической модели, объясняющей развитие как процесс замещения продукта (модель S-кривой) [33]. Фазы жизненного цикла продукта отражают распространение инноваций – прогресс инноваций продуктов / процессов на стадиях внедрения, роста, зрелости и спада. Учитывая конкурентную среду инновационного / диффу-

зионного процесса в отрасли, Уттербек и Абернати [32] разработали модель динамики инноваций – модель жизненного цикла инноваций – для описания процесса инноваций и степени технологических изменений, а также возможности технологического прогнозирования.

В теориях экономического роста и технологических изменений Абернати, Кларк и Кэнтроу [34] приводили доводы в пользу того, что процесс промышленной зрелости является движущей силой развития отрасли. Они рассмотрели природу инновационного процесса, а также конкурентную среду, в которой развиваются технологии, чтобы объяснить прогресс отрасли. Что касается эволюционного теоретизирования экономического роста, они утверждали, что технологические изменения могут изменить характер инноваций и конкуренции и со временем повлиять на структуру отрасли.

Таким образом, проведенный анализ показал, что технологическое развитие и инновации неразрывно связаны с экономической системой и, следовательно, с изменениями, неравенством и взаимодействиями в этой системе. Вместе с тем на разработку, развитие и внедрение новых технологий влияет инновационная экосистема, которая, в свою очередь, находится под влиянием меняющихся технологий и институтов [35]. Как отмечает И. В. Новикова [36], формируется сетевая экономика, представляющая собой «экосистему взаимоотношений между традиционными факторами производства, объединенными единой информационной средой, и приводящая к снижению транзакционных издержек за счет применения цифровых технологий. Появляется принципиально новая экономическая система и новая совокупность производственных, экономических отношений. Их новизна заключается в алгоритмизации экономических отношений». Развите сетевой экономики приводит к «…конкуренции новых экосистем – конкуренции интегрированных между собой цифровых платформ».

Важной идеей, объединяющей пространственно-временные измерения теории технико-экономической парадигмы, является идея технологических траекторий в национальных инновационных системах [5]. Идея траекторий в национальных инновационных системах (разработанная, например, с помощью сравнительного анализа по странам, в том числе Нельсоном [37]) говорит о том, что каждая страна следует своим собственным путем развития в общих рамках существующей технико-экономической парадигмы, а также – и это очень важно – под влиянием прошлой истории и конкретных условий местного контекста.

Следует отметить, что в контексте управления технологиями термин «инновация» имеет несколько контекстуальных определений: 1) как процесс совершенствования существующих технологий [14, 16]; 2) как процесс превращения возможностей в практическое использование [38, 39]; 3) как интегрированный процесс расширения технологической границы, превращения ее в лучшие коммерческие возможности и реализации коммерциализированной инновации продукта / процесса на конкурентном рынке с широким использованием [40, 41].

В отдельную категорию в экономической литературе выделяются системные инновации, как определенный тип инноваций, для реализации которого требуется ряд взаимодополняющих систем. Это набор взаимосвязанных инноваций, и в соответствии с ними для достижения признания на рынке необходима инновационная коалиция [42, 43]. Многие финансовые инновации являются системными (например, кредитные карты, международная электронная система платежей, смарт-карты для финансовых приложений) [44].

Технологические инновации являются основой инновационной экономики [45]. Новые продукты, услуги и знания предоставляют средства для создания ценности, решения проблем и повышения качества жизни. Технологические инновации можно условно разделить на два типа: 1) революционные, прерывистые, прорывные, радикальные, срочные (emergent) технологии; 2) эволюционные, непрерывные, поступательные технологии [46, 47, 48].

В современной российской экономической науке следует выделить работы Д. С. Львова и С. Ю. Глазьева. На основе сравнительного анализа долгосрочного технико-экономического развития различных государств исследован опыт централизованного управления этим процессом [49]. Предложены подходы к формированию новых технико-экономических парадигм на основе теории циклической динамики и инноватики, на трех уровнях: микроуровень – совершенствование моделей и модификаций промышленной продукции и ее качественных характеристик с учетом новых технологий и инноваций, мезоуровень – десятилетний цикл смены технологий, обновления производственных фондов; макроуровень – пятидесятилетний цикл смены технологических укладов [50]. Технологический уклад обладает сложной внутренней структурой, состоящей из элементов различного функционального значения. Комплекс базисных совокупностей технологически сопряженных производств

образует ядро технологического уклада. Технологические нововведения, определяющие формирование ядра технологического уклада и революционизирующие технологическую структуру экономики, получили название «ключевой фактор». Отрасли, интенсивно использующие ключевой фактор и играющие ведущую роль в распространении нового технологического уклада, являются его несущими отраслями [51].

Кристенсен и Бауер утверждали, что именно прорывные технологии вызывают изменения в существующей структуре рынка и доминирующих фирмах [52]. По определению Кристенсена, прорывные технологии – это, по сути, коммерческие сбои на существующем рынке, на который внедряется новый продукт или услуга (технология). В основе прорывных инноваций лежат три теории [35]: 1) теория разрушительных инноваций, в которой новые организации используют «простые и удобные недорогие инновации для обеспечения роста и победы над влиятельными соперниками»; 2) теория ресурсов, процессов и ценностей, которая объясняет, что эти три компонента совместно определяют сильные и слабые стороны фирмы; 3) теория эволюции цепочки создания стоимости, предполагающей, что компании необходимо напрямую контролировать свою цепочку создания стоимости и решать проблемы, которые в противном случае помешали бы этой фирме захватить стоимость из своей деятельности.

Прорывные технологии могут быть классифицированы как подрывные, когда они свергают существующие (или широко принятые) научные парадигмы, идеи или методы [17]. При этом подрывной характер новых технологий может формироваться не столько от разрушения рынка или существующих технологических парадигм, сколько от разрушения существующей модели рыночных систем, организационных структур или социального взаимодействия. Предсказание типа разрушения может быть трудной задачей в сложной системе, такой как инновационная система, так как обратные связи и эффекты не являются линейными [53].

В этой связи в экономической литературе выделяется несколько уровней разрушения под воздействием прорывных технологий [45].

1. Разрушения первого порядка – это локальное изменение на рынке или в отрасли (теория прорывных технологий Кристенсена, разрушения на микроуровне).

2. Разрушения второго порядка – это технологические разрушения, распространяющиеся в обществе, создающие масштабные изменения, нарушающие социальные взаимодействия и отношения, организационные структуры, институты, государственную политику и (иногда) физическую среду (теория длинных волн Кондратьева [54, 55]) (разрушения на макроуровне). Разрушения второго порядка, хотя и достигают большего, чем разрушения первого порядка, не являются длинными волнами, потому что имеют более короткий цикл. Они вызваны взаимодействием прорывных технологий первого порядка в сложной инновационной экосистеме.

В данном контексте важно отметить концепцию «Технологии общего назначения» (GPT), которая является ключевым фактором в появлении новых технологических экосистем [56, 57]. Определение GPT, предложенное Липси [58], имеет четыре наблюдаемые характеристики, а именно: 1) это единая, уникальная универсальная технология; 2) изначально есть много возможностей для улучшения, хотя она широко используется в отрасли; 3) имеет много разных применений; 4) создает много побочных эффектов. GPT по своему совокупному экономическому воздействию [59] может быть как эндогенным, так и экзогенным для экономической системы [58]. GPT может быть продуктом, процессом или организационной системой. При наличии общеэкономических эффектов GPT со временем улучшаются и порождают другие инновации, поскольку изобретение в одной области запускает открытия и создает возможности в иных областях [60]. По мнению ученых, существует более 20 различных видов известных GPT, таких как колесо, паровой двигатель или заводская система. Характерной чертой стимулирующих технологий и GPT является то, что существуют большие положительные побочные эффекты двух видов: статические и динамические [61]. Статические побочные эффекты – это стандартные внешние эффекты, которые не приводят к каким-либо изменениям в поведении других экономических агентов. Динамические внешние эффекты возникают, когда инновация изменяет текущую и будущую ценность существующих технологий, а также открывает дополнительные технологические возможности для других агентов. Эти обстоятельства затрудняют получение прибыли от инноваций.

В 1992 году Рабочей группой национальных экспертов по вопросам науки и технологий ОЭСР (NESTI) было разработано

«Руководство Осло» [62], призванное обеспечить международную сопоставимость и соответствующую цифровую платформу для исследований и экспериментов по измерению инноваций. При этом термин «инновация» разделяется на инновационную деятельность и результат инновационной деятельности. Согласно «Руководству Осло», инновация – это новый или улучшенный продукт либо процесс (или их комбинация), который стал доступным для потенциальных пользователей (продукт) или введен в действие единицей (процессом). Инновационная деятельность включает в себя всю деятельность по развитию, финансовую и коммерческую деятельность, осуществляемую фирмой, которая должна привести к инновациям для фирмы. Бизнес-инновация – это новый или улучшенный продукт либо бизнес-процесс (или их комбинация), который значительно отличается от предыдущих продуктов или бизнес-процессов фирмы и который был представлен на рынке или введен в действие фирмой [62]. Актуальное издание «Руководства Осло» дифференцирует инновации в рамках бизнес-процесса, выделяя производство товаров и услуг, логистику и распределение, маркетинг и продажи, информационно-коммуникационные технологии (ИКТ), администрирование и управление, развитие продуктового и бизнес-процессов.

Вместе с тем по уровню проникновения, влияния и «подрывного воздействия» на все сферы человеческой деятельности безусловным лидером является именно направление ИКТ. При этом по мере того, как ИКТ первого порядка разрабатываются и объединяются в кластеры, возникают технологические сбои второго порядка [45]. Среди потенциально подрывных ИКТ второго порядка выделяют такие, как аддитивное производство, адаптивная архитектура безопасности и кибербезопасность, искусственный интеллект (AI) и машинное обучение (ML), дополненная и виртуальная реальность, автономные автомобили, Блокчейн; электронные платежи; цифровая (крипто) валюта, облачные вычисления, цифровые и социальные сети, Big Data Analytics (аналитика больших данных), цифровое удостоверение личности, цифровые близнецы, FinTech, IoT (Интернет вещей), цифровые платформы, робототехника, умные / интеллектуальные системы; умная инфраструктура; Smart Grid (умные энергосети); Smart City (умные города); умные домашние технологии.

Важно выделить системы технологических инноваций (technological innovation system TIS), которые включают взаимодействие и координацию между различными субъектами из разных институциональных сфер [63, 64, 65]. Поэтому TIS придерживается целостного подхода к пониманию взаимодействия между различными участниками и функциями, которые влияют на генерацию, распространение и использование новых технологий [65, 66]. В рамках данной исследовательской традиции функциональная инновационная система принимает динамическую характеристику процесса технологических изменений [67]. Этот подход помогает проанализировать взаимодействие между различными функциями инноваций и ключевыми участниками, которые влияют на скорость, направление и конечный успех инноваций.

На национальном уровне, изучая проблематику построения системы инноваций, Лундвал и Нельсон [19, 68, 69] обосновали тезис о том, что системы инноваций следует рассматривать не только в узком смысле институтов НИОКР, но и в широком контексте встроенности инновационных систем в социально-экономическую систему, целесообразности детального изучения роли инноваций в национальных, региональных экономиках, отраслевых системах [19]. Концепция национальной инновационной системы (NIS) относится к интерактивной системе учреждений, частных и государственных фирм, университетов и правительственных учреждений, направленных на производство, распространение и эксплуатацию знаний в рамках национальных границ [70]. Взаимодействие может быть достигнуто с помощью рыночных и нерыночных механизмов, таких как сотрудничество и долгосрочные сетевые соглашения в рамках отношенческого контракта. Концепция NIS является динамичным инструментом для исследования, формулирования, планирования и позиционирования национального экономического и социального развития с использованием технологий и инноваций в качестве основной движущей силы [68, 71, 72].

Фримен определял Национальную инновационную систему как «сеть учреждений в государственном и частном секторах, чья деятельность и взаимодействие инициируют, импортируют, модифицируют и распространяют новые технологии» [64, 73]. Эта парадигма формирует условия для инновации в конкретном национальном институциональном контексте, в которых участники на разных уровнях находятся в постоянном взаимодействии. Именно эти взаимодействия

составляют основу системы, и они определяются такими факторами, как культура, нормы, институциональные механизмы и государственная политика [37]. Фирмы являются основными инновационными субъектами, поскольку у них имеется стимул осуществлять поиск, хранить и накапливать инновационные возможности. Однако на способность фирм к инновациям влияет взаимодействие с широким кругом внешних организаций, государственных и частных субъектов, поставщиков, клиентов, рынков и т. д. [74].

В этом контексте государство играет важную роль в стимулировании способности предприятий внедрять, совершенствовать и создавать новые технологии, а также отвечает за обеспечение инфраструктуры и создание соответствующей институциональной платформы для обмена знаниями и их распространения [75]. Правительство, в свою очередь, как институт призвано руководить инвестициями в образование и профессиональную подготовку, а также исследованиями [76].

За последние несколько десятилетий появилось большое количество системно-инновационных подходов для объяснения инноваций в сложных конкурентных средах [77]. При этом концептуальная модель «Система доставки технологий (Technology Delivery System – TDS)» была впервые предложена в 1970-х годах и предполагает техноцентрический подход для понимания того, что превращает идею в эффективную инновацию. В данной модели инновационный процесс стимулируется рынком, на котором правительство пытается минимизировать барьеры, препятствующие TDS, и поддерживать борющиеся отрасли с помощью инновационной политики устранения рыночных сбоев [78]. Каждая технология имеет свою собственную систему доставки, состоящую из ряда интерактивных компонентов, и каждый компонент состоит из набора институтов, которые способствуют выполнению общей функции. Эти учреждения могут включать исследовательские институты, производственные фирмы, компании по распространению продукции или кредитные учреждения, которые предоставляют операционные средства другим компонентам в TDS [79]. Венк и Куен предложили структуру TDS, включающую четыре элемента (вводные данные, государственные и частные институты, посреднические институты и результаты) для прогнозирования важных факторов, связанных с конкретной инновацией [80]. TDS изображает инновационный процесс как поток действий, обусловленный изобретением

новых возможностей и вызванный спросом на продукты, и на этот процесс большое влияние оказывают различные внешние воздействия общества, например государственная политика [81].

Ицковиц и Лейдерсдорф предложили теорию тройной спирали, которая рассматривает коллективную роль трех действующих лиц в производстве технологий – правительства, промышленности и научных кругов [82]. Караянис и Григорудис развили данную модель, предложив четыре составляющие спирали (четырехзвенная модель инновационной деятельности): система образования, включая академические учреждения, университеты, системы высшего образования и школы (человеческий капитал); экономические системы, охватывающие сектора экономики, фирмы, сектор услуг и банки (экономический капитал); политическая система, которая определяет направления движения государства в настоящем и будущем, законы и т. п. (политический и правовой капитал); гражданское общество (в его основе лежат СМИ и культура, которые в совокупности образуют две формы капитала: социальный и информационный) [83].

Каллон была предложена концепция технико-экономических сетей, в рамках которой объектами выступают: исследования, производство технологий, финансы и управление / регулирование, а субъектами: артефакты и элементы, связывающие эти объекты в сеть. При этом технико-экономические сети могут быть на уровне отдельного проекта (микро) или на уровне отраслей (мезо) [84, 85].

Быстрое развитие ИКТ повлияло на принятие и использование этих технологий [86]. Ученые, изучающие информационные системы управления (Management information systems – MIS), разработали ряд моделей, направленных на анализ влияния цифровых технологий на различные процессы [87, 88]. Так, концепция индивидуального принятия технологий была введена в литературу по информационным технологиям Дэвисом с его моделью принятия технологий (Technology acceptance model – TAM) в целях изучения индивидуального поведения при принятии и внедрении ИТ. Это исследование было сосредоточено на двух конструкциях: воспринимаемой полезности и воспринимаемой простоты использования [89, 90].

На уровне фирмы большинство исследований по внедрению технологий основаны на теории Торнацкого и Флейшера «Технологии, организация и среда» (Technology, organization and environment – TOE) [91].

Кроме того, Венкатеш разработал «Единую теорию принятия и использования технологии» (Unified theory of acceptance and use of technology – UTAUT) для объяснения индивидуального поведения при использовании технологии, предполагающую четыре основных конструкта – ожидаемая производительность, ожидаемое усилие, социальное влияние и способствующие условия, являющихся прямыми детерминантами поведенческого намерения и, в конечном счете, поведения. Им также предложена модель принятия и технологий в домашних хозяйствах (Model of adoption and technology in households – MATH) [92].

TTF (Task-technology fit) – теоретическая модель соответствия задач технологиям для изучения взаимосвязей между информационными системами и индивидуальными характеристиками, которая зависит как от задачи, так и от технологических характеристик и непосредственно связана с производительностью и конечными пользователями [93, 94]. RBV (Resource-based view) – это модель управления, используемая для регулирования планируемых ресурсов с потенциалом предоставления сравнительного преимущества фирме [95].

К классическим теориям, объясняющим поведение человека, связанным с внедрением новых цифровых технологий, также относятся «Теория рационального действия» (Theory of Reasoned Action – TRA), разработанная Айзеном и Фишбайном [96, 97], и «Теория планового поведения» (Theory of Planned Behavior – TPB), предложенная Айзеном [98]. TPB была расширена за счет добавления новой конструкции, воспринимаемого поведенческого контроля, который теоретически считается дополнительной детерминантой намерения и поведения [99].

В данном контексте следует также отметить исследовательскую работу Веблена, в которой он описал врожденный консерватизм социальных структур в отношении интеграции технологических инноваций, введя термин «церемониальная инкапсуляция» [100, 25], которая описывает ограничения в адаптации технологии к уже существующим институциональным структурам. Церемониальные ценности остаются инертными, даже обращенными назад, несмотря на тягу от новой технологии к прогрессу и эффективности. Акцент на консерватизме институциональных структур и вдохновляющих их ценностей обеспечивает важное понимание механизма институциональной перестройки и социализации технологических инноваций.

Заключение

Таким образом, волнообразный процесс технологических инноваций оказывает формирующее влияние, задающее новую динамику в экономических условиях, институциональной и социальной сферах, стимулируя сдвиг в технико-экономической парадигме. Анализ теоретических подходов показал консенсус в отношении концепции подрывного характера технологических инноваций относительно экономической системы, которые приводят к масштабным изменениям, нарушающим социальные взаимодействия и отношения, организационные структуры, институты, государственную политику. В результате смены технико-экономической парадигмы может потребоваться новая институциональная структура для поддержания последующего развития. В современной экономике технологическим синонимом институциональной структуры можно отчасти считать экосреду, которая интегрирует традиционные факторы производства в рамках общей алгоритмизированной информационной среды и направлена на оптимизацию затрат, повышение качества и комплексности предоставляемых услуг. На страновом уровне формируется концепция национальной инновационной системы, встроенной в социально-экономическую систему государства, в которой взаимодействия определяются такими факторами, как культура, нормы, институциональные механизмы и государственная политика.

1.2. Анализ категории «цифровая экономика» с элементами системной методологии

Технологии на основе ИКТ оказывают разрушительное воздействие на многие отрасли, предприятия и сферы деятельности, в том числе производство, связь, торговлю, научные исследования, финансовые системы, в частности из-за сбоев первого и второго порядка, которые, как отмечено в предыдущей подглаве, имеют проявления как на локальном (микроуровне), так и на мкроуровне, нарушая социальные взаимодействия и отношения, организационные структуры, институты, государственную политику. В результате разработки и внедрения ИКТ технологий, социально-экономического и политического развития общества происходят значительные изменения в инновационной экосистеме. В данном контексте важно методологически правильно определить понятие «цифровая экономика», ибо именно она лежит в основе понятия «новая экономика».

Процесс расширения использования ИКТ в экономике и других сферах деятельности человека получил название «цифровизации». Данный процесс характеризуется не только переходом от аналогового к цифровому, от печатного к электронному или беспроводному [101]. Цифровизация – общий термин для обозначения тенденции и воздействия растущего использования цифровых технологий. Термин «цифровой» происходит от латинского слова digital [102][1].

Цифровое развитие – процесс последовательной цифровой трансформации экономической деятельности и государственного управления. Данный этап является закономерным переходом от общей компьютеризации деятельности, предусматривающей оснащение компьютерным оборудованием, проведение автоматизации и информатизации экономической деятельности и государственного управления, к углублению цифровых преобразований – осуществлению цифровой трансформации, которая проявляется в качественных изменениях, заключающихся как в отдельных цифровых преобразованиях, так и в принципиальном изменении структуры экономики, переносе центров создания добавленной стоимости в сферу информационных ресурсов и сквозных цифровых процессов.

Цифровизация может рассматриваться в трех измерениях: 1) в сфере бизнеса она относится к операциям, связанным с формированием, оптимизацией и преобразованием бизнес-процессов, функций, моделей, видов деятельности с использованием цифровых технологий. Цифровизация рассматривается как шаг к развитию цифрового би знеса и цифровым инновациям, а также к созданию новых цифровых потоков дохода и предложения. «Оцифрованная» информация и знания становятся одним из факторов производства [103]; 2) использование в конкретной среде, например в создании «цифрового рабочего места», которое включает в себя квалифицированную рабочую силу и цифровые инструменты (такие как мобильные устройства, унифицированные коммуникационные платформы); 3) внедрение цифровых технологий по всем направлениям социальной и гуманитарной деятельности [104].

Цифровизация создает новые цифровые возможности, которые оказывают преобразующее влияние на организацию экономической деятельности, поддерживая радикальные инновации в бизнес-

[1] В информационных технологиях термин «цифровой» относится к двоичной системе вычисления, которая была принята в середине XX века в качестве основной логики для вычислительных машин.

моделях [105, 106]. Согласно определению Тильсона, цифровизация – это социо-технический процесс применения методов оцифровки в более широком социальном и институциональном контексте, который делает цифровые технологии инфраструктурными [107]. По мнению Миллера [108], цифровизация способствовала созданию совершенно новых цифровых рынков, управляемых платформенными предприятиями на основе открытой бизнес-модели, позволяющей связываться и взаимодействовать друг с другом и внешним потребителям, и производителям. Организация экономического сотрудничества и развития (ОЭСР) отмечает, что стремительный рост вычислительной мощности оборудования, емкости для хранения данных и скорости связи создали условия для появления обширной и разнообразной экосистемы технологий [109].

Цифровизация включает три фазы: оцифровка, цифровизация и цифровая трансформация [110].

Согласно определению Юу, оцифровка – это кодирование аналоговой информации в цифровой формат, которое делает физические продукты программируемыми, адресными, осмысленными, передаваемыми, запоминающимися, отслеживаемыми и ассоциируемыми [111]. ОЭСР трактует его как интеграция цифровых инструментов для выполнения существующих задач [109].

В экономическом контексте на микроуровне цифровизация направлена на использование цифровых технологий для повышения эффективности за счет снижения затрат и рисков или изменения модели бизнеса в процессе создания новых продуктов и услуг и новых источников дохода. Цифровизация позволяет компаниям напрямую взаимодействовать с людьми через социальные сети, оценивая реальные потребности и поведение людей, потенциально влияя на их предпочтения.

Цифровые технологии основаны на коде, который можно изменять, обновлять, исправлять, взламывать, хранить и анализировать без изменения самой физической машины [112]. Программируемая и перепрограммируемая природа цифровых технологий, а также возможность сбора и анализа данных придают больше возможностей цифровым технологиям. Кроме того, гибкость и адаптивность кода более тесно связывают людей с машинами, создавая новые формы совокупностей между людьми и нечеловеческими субъектами. Цифровые технологии порождают так называемую четвертую промышленную революцию [113] и цифровую трансформацию [114], поскольку они позволяют или усиливают беспрецедентную

конвергенцию компьютеров, коммуникаций, контента и сетей, людей [115, 116].

Цифровая трансформация, согласно Фицджеральду, Крушвицу, Бонне и Уэлшу [117], – это использование новых цифровых технологий (социальных сетей, мобильных устройств, аналитики или встроенных устройств) для обеспечения значительных улучшений в бизнес-процессах, таких как повышение качества обслуживания клиентов, оптимизация операций или создание новых бизнес-моделей. Лью, Чен и Чоу утверждают, что цифровая трансформация – это организационная трансформация, которая объединяет цифровые технологии и бизнес-процессы в цифровой экономике [118]. Роджерс рассматривает цифровую трансформацию не в контексте технологии, а как стратегию предприятия, направленную на извлечение выгоды из новых инноваций бизнес-модели, которые оптимизируют потребности и опыт клиентов [119].

Цифровая трансформация связана с изменениями, которые цифровые технологии могут вызвать в бизнес-модели компании, что приводит к изменению продуктов или организационных структур либо автоматизации процессов [120]. Цифровая трансформация – это комбинированное воздействие нескольких цифровых инноваций, приводящих к появлению новых действующих лиц, структур, практик, ценностей и убеждений, которые изменяют, заменяют или дополняют существующие правила игры в организациях, экосистемах, отраслях [121]. В 2008 году Ланкшир и Кнобель предложили определение цифровой трансформации как достижимой цели, предполагающей такое использование цифровых технологий, которое обеспечивает инновации, творческий подход и стимулирует существенные изменения в области профессиональной деятельности или знаний. Вестерман также определяет цифровую трансформацию как использование технологии для радикального повышения производительности или охвата предприятий [122, 123]. Суть трансформации заключается не только во внедрении технологий нового века, но и в способности организации переосмыслить возможности, включая расширение, взаимодействие, конвергенцию, модульность и интеграцию распространенного бизнеса с цифровыми технологиями. Международная финансовая корпорация (МФК) определяет цифровую трансформацию как непрерывный процесс, посредством которого предприятия или приспосабливаются к своим клиентам и рынкам (внешней экосистеме), используя цифровые компетенции для создания новых бизнес-моделей, продуктов и услуг,

или он приводит к разрушительным изменениям [124]. В докладе Всемирного банка о мировом развитии 2016 года перечислены следующие дивиденды, получаемые от цифровой трансформации: рост производительности труда; повышение конкурентоспособности компаний; снижение издержек производства; создание новых рабочих мест; более полное удовлетворение потребностей людей; преодоление бедности и социального неравенства [125, 126].

Руан выделила следующие характеристики цифровизации [104].

1. Скорость. Оцифровка привела к ускорению экономической деятельности. В цифровом пространстве транзакции между конечными пользователями в различных юрисдикциях могут быть осуществлены без потери времени и цифрового контента, к ним возможен немедленный доступ с любого устройства, подключенного к Интернету.

2. Трансграничная экономика масштаба. Цифровой рынок предоставляет возможность цифровым продуктам и услугам получить глобальное распространение. Экономическая деятельность, происходящая на цифровых рынках, нарушает традиционные границы юрисдикции, создавая многогранные вызовы глобальным нормативно-правовым рамкам.

3. Растущее влияние нематериальных активов, в особенности прав интеллектуальной собственности.

4. Важность цифровой информации, участия пользователей, сетевых эффектов и синергии, включая интеллектуальную собственность. При этом конкурентные преимущества от анализа данных возрастают с увеличением объема собранной информации, связанной с конкретным пользователем или клиентом.

5. Слияние технологий, которые стирают границы между цифровым и физическим миром.

6. Внешнее потребление. На цифровых рынках дополнительная полезность от потребления определенного товара или услуги зависит от количества других пользователей, приобретающих этот же товар или услугу. Данный эффект называется прямым внешним эффектом сети. Внешнее потребление является основным драйвером роста платформ.

7. Косвенные сетевые эффекты возникают в контексте многосторонних рынков, когда определенная группа конечных пользователей (пользователей социальной сети) извлекает выгоду от взаимодействия с другой группой конечных пользователей (рекламодателями в социальной сети) через онлайн-платформу.

8. Эффекты блокировки и конкуренции. Цифровые транзакции выполняются на разных электронных устройствах, которые используют разные операционные системы. В результате клиенты могут быть привязаны к конкретной операционной системе после приобретения конкретного устройства.

В данном контексте цифровые технологии (рассматриваемые как комбинация информационных, вычислительных, коммуникационных технологий) коренным образом меняют бизнес-стратегии, бизнес-процессы, возможности компаний, продукты и услуги, а также ключевые межфирменные отношения [127]. Они позволяют снижать стоимость хранения, вычислений и передачи данных, включая: затраты на поиск, затраты на репликацию, транспортные расходы, расходы на отслеживание и проверку [128].

Проведенный анализ показал, что в современной экономической литературе цифровые бизнес-стратегии могут быть классифицированы 1) как область применения стратегии цифрового бизнеса, 2) масштаб стратегии цифрового бизнеса, 3) гибкость стратегии цифрового бизнеса с точки зрения выполнения и непрерывности и 4) источники создания стоимости бизнеса [127, 129]. Выбор той или иной цифровой стратегии зависит от институциональных экосистем, намеревающихся использовать цифровые возможности для создания стоимости, интеграции процессов и функций. Масштаб и скорость реализации цифровой стратегии зависят от величины использования сетей и экосистем для инноваций [130].

Цифровые технологии проявляются в различных формах, таких как цифровые продукты или услуги [113, 131], цифровые платформы [132], цифровые инструменты и инфраструктура [133], цифровые артефакты [134] и инновации в услугах с использованием Интернета [135]. Концепция цифровых технологий была описана как результат трех отдельных, но взаимосвязанных элементов: цифровых артефактов, цифровых инфраструктур и цифровых платформ [136]. Цифровая инфраструктура – цифровые технологии, устанавливающие стандарты, позволяющие, ограничивающие и координирующие действия и взаимодействия различных участников экосистем [137, 138, 139]. Прототипом этого вида инфраструктуры является продуктовая платформа. В продуктовых платформах несколько действующих лиц в экосистеме играют разные роли в процессе создания новых инноваций, производства или предоставления продуктов и услуг.

Инструменты и системы цифровых технологий (например, облачные вычисления, аналитика Big Data, онлайн-сообщества, социальные сети, 3D-печать, цифровые близнецы и т. д.), которые предлагают коммуникационные возможности, сотрудничество и/или вычислительные возможности для поддержки инноваций и предпринимательства. Цифровой артефакт – это цифровой компонент, приложение или мультимедийный контент, который является частью нового продукта (или услуги) и предлагает определенные функции или ценность для конечного пользователя [140]. Цифровые блоки – общепринятые, готовые или настраиваемые модули, охватывающие наборы цифровых технологий для запуска продукта, услуги или создания организации [141, 142, 143].

Цифровые активы, как отмечает Руан, представляют собой активы в цифровой форме, утрата которых приведет к экономическим потерям для его владельца [104]. Подобно традиционным ресурсам, цифровые активы обычно имеют жизненные циклы, охватывающие этапы создания, управления, распространения и сохранения, могут иметь материальную и нематериальную форму. Нематериальные цифровые активы – это информационные активы, выраженные в дискретной числовой форме для использования вычислительным устройством. Более поздние определения информационных активов описывают его как зонтичную категорию, включающую в себя данные, информацию и явные знания, которые управляются как единое целое, чтобы их можно было понимать, совместно использовать, защищать и эффективно использовать. В контексте информационного риска информационный актив – это ресурс, который должен защищаться контрмерой, предусмотренной политикой безопасности информационной системы. Цифровые активы предоставляют возможность предоставлять услуги, принимать более правильные решения, повышать производительность и достигать конкурентных преимуществ, а также могут продаваться напрямую как отдельный продукт [144]. К отдельным видам сетевых активов можно отнести системные активы, программные активы, оборудование, сервисные активы, роботизированные активы, активы данных и метаданных, устройства с цифровой поддержкой.

Как отмечают Муди и Уолш, цифровые активы демонстрируют атрибуты традиционных экономических товаров [144].

1. Активы данных дают возможность предоставлять услуги и принимать эффективные решения.

2. Если организация владеет активами данных, она имеет к ней доступ, если только она не продает или не предоставляет доступ другой стороне.

3. Активы данных обычно собираются как побочный продукт произошедших транзакций (внутреннее развитие), или могут быть результатом покупки (например, собственной почтовой базы данных) либо открытия (например, путем анализа данных).

Одним из фундаментальных отличительных признаков цифровых активов по сравнению с традиционными активами является то, что они не обязательно являются «дефицитными», так как многие типы цифровых активов мгновенно масштабируются и не являются конкурирующими. Уникальными характеристиками цифровых активов (по сравнению с традиционными) являются:

1) совместное использование нематериальных цифровых активов имеет тенденцию к увеличению их стоимости;

2) дублирование информации не добавляет новой ценности, но добавляет дополнительную стоимость;

3) производство и распространение цифровых активов влечет за собой более высокие фиксированные затраты и более низкие переменные затраты;

4) цифровые активы могут распространяться через многосторонние рынки;

5) безграничный характер цифровых активов.

Важно отметить, что в отличие от традиционных экономических товаров и услуг, которые классифицируются в соответствии с международно признанными стандартами, такими как Ниццкая классификация, не существует общепризнанной классификации цифровых товаров и услуг, которые можно использовать для контроля их себестоимости и рыночной стоимости.

В экономической литературе важным атрибутом адаптивности систем к цифровым технологиям является понятие «цифровой гибкости» (Digital agility), характеризующее способность субъектов экономики находить и использовать рыночные возможности, предоставляемые цифровыми технологиями [110, 145]. Предприятия должны быть гибкими в цифровом отношении, чтобы постоянно модифицировать и реконфигурировать существующие цифровые активы и возможности [146].

Накопление цифровых компетенций (информации, связей, безопасности, контента) и цифровых технологий формирует цифровой

капитал предприятий [147]. Цифровой капитал отличается от определения «информационного капитала», которое Бордо представил в своих более поздних работах как капитал знаний [148].

Для обозначения создания новых предприятий и преобразования существующих предприятий путем разработки новых цифровых технологий или экспериментального использования новых технологий была введена концепция цифрового предпринимательства для обозначения создания новых и преобразования существующих предприятий путем разработки новых цифровых технологий или экспериментального использования новых технологий [149, 150, 151]. Цифровое предпринимательство также известно как кибер-предпринимательство, поскольку оно относится к использованию Интернета и технологических платформ для управления и выполнения деловых операций с клиентами, посредниками или партнерами [152] и реализации цифровых продуктов или услуг с помощью электронных сетей [153]. Цифровое предпринимательство представляет собой важнейшую опору для цифрового экономического развития [151] и подчеркивает необходимость реализации возможностей, основанных на цифровых медиа и технологиях [154], через основную бизнес-модель, использующую три ключевых компонента, таких как маркетинг, транзакции и сервисная поддержка [155]. Цифровое предпринимательство также определяется как подкатегория предпринимательства, в которой часть или все, что было физическим в традиционных условиях, оцифровано на основе использования цифровых медиа и технологий [156]; создание новых предприятий и трансформация существующих предприятий путем разработки новых цифровых технологий или экспериментов с новым использованием таких технологий [149, 150].

Комплексное изучение влияния ИКТ на экономические системы, их адаптацию и трансформацию под воздействием цифровых инноваций привело к созданию концепции «цифровой экономики», которую в 1995 году сформулировал Тэпскотт [157]. Подчеркнуто влияние цифровизации на три ключевые сферы государств: правительство, рынок и гражданское общество, что приводит к их фундаментальным изменениям по мере распространения сетевых технологий [158].

Оверби и Аудестад предложили рассмотрение цифровой экономики, как экономики, основанной на цифровых товарах и услугах, чей бизнес-ландшафт сформирован такими технологиями, как социальные сети, мобильные приложения, облачные вычисления, запоминающие устройства, криптовалюты и сервисы обмена [159].

Бухт и Хикс [160], предложили подход к классификации цифровой экономики, принятый за основу Конференцией ООН по торговле и развитию (ЮНКТАД), в рамках которого она рассматривается как часть общего объема производства, которая целиком или в основном произведена на базе цифровых технологий фирмами, бизнес-модель которых основывается на цифровых продуктах или услугах. Таким образом, оно охватывает основные виды деятельности в сфере ИТ («цифровой сектор») и направления экстенсивного применения ИКТ в экономике (рис. 1.1).

Организация экономического сотрудничества и развития (ОЭСР) определяет цифровую экономику как цифровую инфраструктуру, состоящую из технологического оборудования и организационных механизмов, включая компьютерное и программное обеспечение, телекоммуникационное оборудование и услуги, Интернет вещей (IoT), компьютерные сети, а также центров обработки данных, производства полупроводниковых приборов, прокладки оптоволоконных кабелей, коммутаторов, ретрансляторов, услуг цифрового консалтинга и услуг по ремонту оборудования [161].

МВФ определяет цифровую экономику как вид деятельности в области цифровизации, включая информационные и коммуникационные технологии, товары и услуги, онлайн-платформы и базирующиеся на платформе виды экономической деятельности [162].

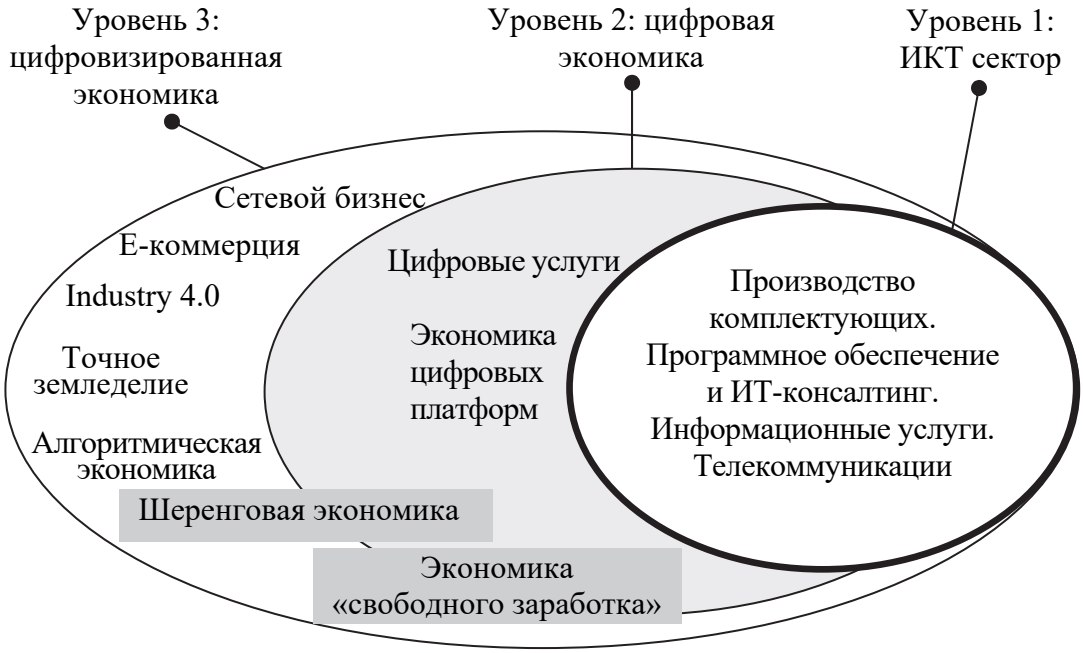


Рис. 1.1. Понятие «цифровой экономики»

В узком смысле цифровую экономику считают разновидностью коммерческой деятельности по производству и продаже электронных товаров и услуг [125]. Соответственно, в нее входит, во-первых, электронная торговля, электронный банкинг и электронные деньги. Во-вторых, цифровая экономика – это сервисы по предоставлению онлайн-услуг, информационные сайты, зарабатывающие на рекламе, Интернет-медиа (звукозапись, кино, пресса, издательская деятельность), развлекательный и деловой контент. В-третьих, в это понятие включается в производство соответствующего оборудования и другие обеспечивающие виды деятельности.

В широком смысле цифровая экономика выступает итогом новой индустриализации (обусловленной внедрением ИКТ – информационно-коммуникационных технологий, или четвертой промышленной революцией) и становления нового технологического уклада – Industry 4.0 [163]. В ее основу входит производство оборудования, использующего ИКТ, и соответствующего программного обеспечения.

Представляется, что в настоящее время формируется принципиально новая экономическая система и новая совокупность производственных, социальных и экономических отношений, новизна которых заключается в их алгоритмизации и платформизации, синергии метатехнологий и цифровых концепций [36]. Вышеназванные экономические концепции являются составной частью более обширного многомерного и комплексного понятия «цифровая экономика».

Базовой единицей системы цифровой экономики является сущность, представляющая собой дуализм программного (цифрового) продукта и цифровых данных (знаний). Рассматривая экономику как область общественных отношений по поводу производства, перераспределения, обмена и потребления, «цифровая экономика» имеет ряд особенностей (табл. 1.5).

Выделяют следующие факторы и характеристики цифровой экономики: 1) новые формы посредничества (on-line платформы) в сфере услуг (peer-to-peer services); 2) стирание границ между производителем и потребителем, а это позволяет конечным потребителям самим становиться производителями (prosumer), что обуславливает переход от экономики производства к экономике потребления; 3) появление новых потребительских товаров длительного пользования, услуг и рост инвестиций; 4) возникновение новых условно бесплатных и субсидированных потребительских товаров и услуг; 5) образование свободных активов, произведенных домашними хозяйствами; 6) рост транзакций в сфере электронной коммерции [157].

Таблица 1.5

Сравнение категорий «экономика» и «цифровая экономика»
(разработано автором)

Категория	Экономика	Цифровая экономика
Производство	Производство – процесс создания материальных и нематериальных благ, которые выступают исходным пунктом экономической деятельности	Производство программных (цифровых) продуктов, генерирование цифровых данных (знаний), которые не только участвуют в прозводственных процессах традиционных отраслей и направлены на их трансформацию, оптимизацию, снижение затрат, но и могут самостоятельно выступать объектом производства, распределения, обмена и потребления
Распределение	Разделение произведенного продукта, дохода между участвующими в его производстве	Распределение связано не только с разделением цифровых товаров и услуг, но и ресурсов и факторов производства (в первую очередь технологий, квалифицированного труда и капитала), доходов в рамках концепции шеринговой экономики. Роль материальных ресурсов и факторов производства значительно снижается
Обмен	Процесс, в котором взамен произведенного продукта люди получают деньги или другой продукт	Обмен связан, как правило, с торговлей нематериальными активами, услугами, знаниями и цифровыми данными. Спецификой цифровой экономики является возможность предоставления цифровых продуктов, услуг по нулевой стоимости. Социальные сети, цифровые платформы, их экосистемы становятся новыми маркетплейсами для обмена информацией и ее потребления
Потребление	Потребление можно разделить на два вида – личное и производственное, или производительное потребление. Личное потребление существует вне сферы общественного производства и является индивидуальным процессом. Производственное (производительное) потребление предполагает использование средств производства, в целях создания новых потребительских благ	Потребление в цифровой экономике программных продуктов и данных (знаний) становится ключевым фактором не только общественной, социальной, но и экономической деятельности. Объектом потребления становятся нематериальные активы – цифровые данные (знания), которые становятся промежуточными товарами (факторами производства) в рамках концепции аддитивного производства. Потребление информации связано с проблематикой цифрового разрыва, так как отсутствие постоянного обучения и переобучения в цифровой сфере является предпосылкой для снижения занятости

К основным особенностям цифровой экономики следует отнести: 1) высокие темпы роста; 2) возможность предоставления товаров и услуг на безвозмездной основе; 3) снижение цен на продукты и услуги ИКТ; 4) цифровые товары являются мобильными и нематериальными, что ведет к существенному изменению бизнес-модели предприятий-производителей; 5) низкие входные барьеры позволяют предприятиям беспрепятственно внедрять инновации; 6) предприятия имеют возможность пользоваться внешними сетями с последующим самораспространением произведенных товаров и услуг; 7) компании биполяризованы между теми, кто уже использует сетевые возможности продаж и теми, кто продолжает применять консервативные бизнес-модели; 8) цифровые компании имеют тенденцию к монополизации своей деятельности.

Ряд экономистов (например, Шапиро, Вериян, Эллисон [164, 165, 166]), подчеркивая роль более низких затрат на цифровую экономику, выявили последствия этих более низких затрат на поиск и транспортировку для промышленной организации в отношении увеличения прибыли, расстояния и двусторонних рынков.

Следует отличать понятие «цифровая экономика» от понятия «сетевая экономика», которая имеет более узкое содержание и представляет собой новую экосистему взаимоотношений между традиционными факторами производства, объединенными единой информационной средой, и приводящую к снижению транзакционных издержек за счет применения цифровых технологий. В экономической литературе также выделяются схожие понятия, включая «информационную экономику», основанную на информации как продукте, который производится и продается; «экономику данных», сфокусированную на аккумулировании и обработке цифровых данных, «интернет-экономику», изучающую экономику интернет-товаров и услуг; «шеринговую экономику, или экономику совместного использования», экономику, в которой люди или организации делятся товарами и услугами (например, посредством таких цифровых платформ, как Airbnb и Uber)[2] [159].

Кроме того, в экономической литературе предложены три базовые регуляторные экономические концепции в рамках парадигмы цифровой экономики: «экономика регулирования», «экономика

[2] Совместную экономику также называют экономикой доступа, одноранговой экономикой, совместной экономикой и краудсорсинговым капитализмом.

платформ» и «экономика экосистем» [167]. Большая часть экономики регулирования основывается на анализе статического равновесия, часто ориентированном на узко определенные рынки. Экономика платформы побуждает аналитиков учитывать соответствующие взаимозависимости между игроками, связанными с платформой. Экосистемный подход учитывает более широкие взаимозависимости, которые влияют на характер и интенсивность конкуренции. Он предполагает, что в динамичной, взаимозависимой системе внешнее регулирование не контролирует результаты полностью, и поэтому могут возникать непреднамеренные, положительные или отрицательные последствия. Кроме того, экосистемный подход обостряет представление о множестве механизмов, которые существуют для управления такими динамическими системами. Оба последних подхода используют адаптивное управление, в котором непрерывный мониторинг результатов используется для тонкой настройки политики. В развитие данных концепций Витт разработал принципы для регулирующих действий на основе структуры, названной emergence economics (формируемой экономикой), которая опирается на отдельные положения экономики инноваций, теории сложных адаптивных систем и экономики экосистем [168].

Важной составной частью понятийного аппарата цифровой экономики является цифровая экосистема. Ли, Ду, Йин определяют ее как самоорганизующуюся, масштабируемую и устойчивую систему, состоящую из разнородных цифровых объектов и их взаимосвязей для повышения полезности системы, уровня взаимодействия и инноваций [169]. Дини, Икании, Манселл определяют ее систему, включающую статическую часть, представленную цифровыми технологиями и людьми, и динамический компонент взаимодействий, формирующих поведение экосистемы [170]. Экосистемы могут быть определены как самоуравновешивающиеся системы слабосвязанных субъектов, взаимодействующих в общей области, в которой взаимодействие сосредоточено вокруг общих ресурсов (товаров, информации, услуг, идей и т. д.). Технологические экосистемы – это те экосистемы, для которых характерна критическая зависимость от конкретных технологий. Общим для данных определений является динамических характер экосистем, определяемый взаимодействующими элементами. С точки зрения

макроэкономики экосистемы являются новыми субъектами экономики, которые формируют гигантские транснациональные рынки товаров и услуг, навязывая правила, регламенты и бизнес-модели как производителям, так и потребителям. Осуществляется новый уровень кастомизации не только потребляемых товаров или услуг, но и самого механизма взаимодействия торговых площадок и конечных потребителей.

Анализ подходов к трактовке понятия «экосистема» в отношении цифровой экономики позволяет рассматривать ее не только как совокупность правил и норм, регулирующих взаимодействие населения, хозяйствующих субъектов, органов государственного регулирования в отношении становления и развития цифровой экономики, но и как определенную алгоритмизацию, последовательность принимаемых норм и правил, которые позволяют наращивать темпы развития, трансформационные формы развития.

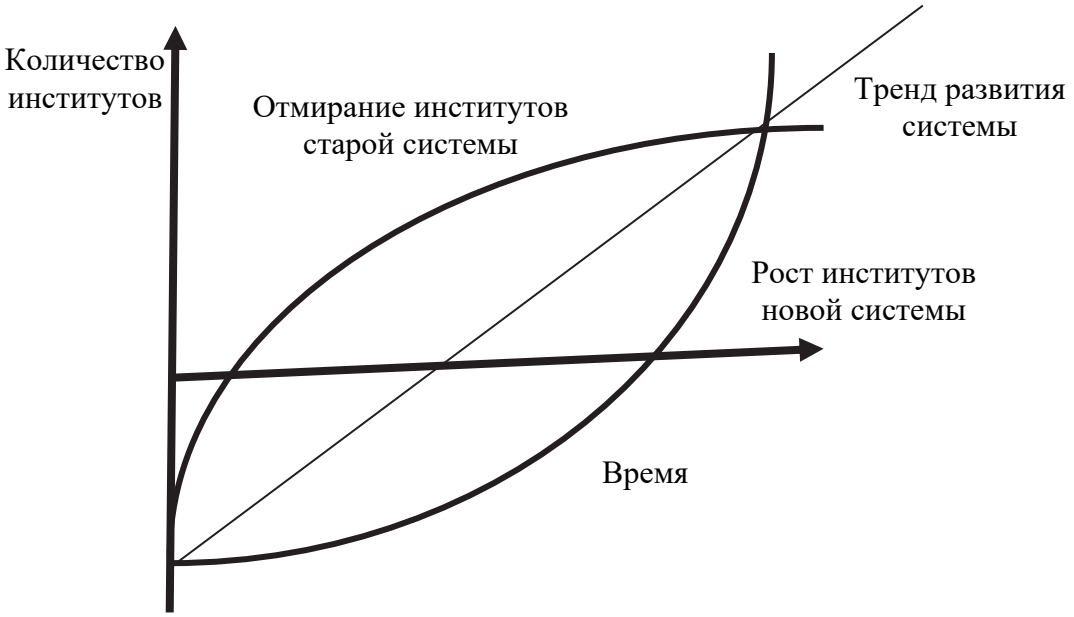


Рис. 1.2. Взаимодействие институтов старой и новой систем, определяющее развитие системы с учетом временных лагов [171]

Схема, приведенная на рис. 1.2, показывает, чем больше угол наклона нижней кривой, тем быстрее идет становление институтов новой системы. Чем более пологий характер у верхней кривой, тем лучше работает» экосистема для новых институтов. Верхняя кривая «толкает» тренд развития системы вниз. А нижняя,

напротив, – вверх. Данная система демонстрирует роль времени в создании институтов и необходимости матрицы формирования новых институтов и отмирания старых.

Заключение

Таким образом, следует отметить, что «цифровизация» является общим термином для обозначения тенденции и воздействия растущего использования цифровых технологий, которые оказывают преобразующее влияние на организацию экономической деятельности, поддерживая радикальные инновации в бизнес-моделях. На микроуровне цифровизация направлена на использование цифровых технологий для повышения эффективности организаций за счет снижения затрат и рисков или изменения модели бизнеса в процессе создания новых продуктов и услуг и новых источников дохода и позволяет компаниям напрямую взаимодействовать с клиентами и поставщиками через сетевые коммуникации.

В настоящее время формируется принципиально новая экономическая система и новая совокупность производственных, социальных и экономических отношений, новизна которых заключается в их алгоритмизации и платформизации, синергии метатехнологий и цифровых концепций. Вышеназванные экономические концепции являются составной частью более обширного многомерного и комплексного понятия «цифровая экономика». Базовой единицей системы цифровой экономики является сущность, представляющая собой дуализм программного (цифрового) продукта и цифровых данных (знаний). Через призму общественных отношений по поводу производства, перераспределения, обмена и потребления «цифровая экономика» имеет ряд отличий от классического подхода, которые могут быть сведены к следующим:

а) в сфере производства – доминирование нематериальной формы производства программных (цифровых) продуктов, генерирование цифровых данных (знаний), которые не только участвуют в прозводственных процессах традиционных отраслей и направлены на их трансформацию, оптимизацию, снижение затрат, но и могут самостоятельно выступать объектом проиводства, распределения, обмена и потребления;

б) распределение связано с разделением не только цифровых товаров и услуг, но и ресурсов и факторов производства (в первую очередь технологий, квалифицированного труда и капитала), доходов

в рамках концепции шеринговой экономики. Роль материальных ресурсов и факторов производства значительно снижается;

в) обмен связан, как правило, с торговлей нематериальными активами, услугами, знаниями и цифровыми данными. При этом спецификой цифровой экономики является возможность предоставления цифровых продуктов, услуг по нулевой стоимости. Социальные сети, цифровые платформы, их экосистемы становятся новыми маркетплейсами для обмена и потребления информации;

г) потребление в цифровой экономике программных продуктов и данных (знаний) оказывается ключевым фактором не только общественно-социальной, но и экономической деятельности. Объектом потребления выступают наматериальные активы – цифровые данные (знания), которые становятся промежуточными товарами (факторами производства) в рамках концепции аддитивного производства. При этом возникает проблема «потребления информации», свзанная с «цифровым разрывом» между поколениями и социальными группами, при котором постоянного обучения и переобучения в цифровой сфере является предпосылкой для нарастания безработицы.

Характеристаками цифровой экономики на текущем этапе ее становления являются следующие: стирание границ между производителем и потребителем; появление новых потребительских товаров длительного пользования, услуг и рост инвестиций; новые формы посредничества; появление новых условно бесплатных и субсидированных потребительских товаров и услуг, свободных активов, произведенных домашними хозяйствами; рост транзакций в сфере электронной коммерции. Кроме того, ключевыми особенностями цифровой экономики являются: высокие темпы роста; снижение цен на продукты и услуги ИКТ, изменение бизнес-моделей предприятий-производителей, низкие входные барьеры на рынок; новые механизмы продвижения товаров, работ и услуг; монополизации деятельности цифровых компаний.

1.3. Становление цифровой экономики: технологические предпосылки, этапы, основные тенденции

Интенсивная цифровизация современной экономики является важнейшим трендом, который предопределяет формирование новых характеристик, актуальных особенностей текущей экономической

системы. Вместе с тем с целью выявления и анализа динамики данных изменений представляется целесообразным выделить основные направления цифровизации, их влияние на текущее и возможное будущее состояние экономики как на национальном, так и международном уровнях.

Ряд исследователей отмечают, что стартовой точкой цифровизации экономики следует считать 1945 год, когда была начата коммерциализация технологий, разработанных во время Второй мировой войны [128, 172]. Вместе с тем ограниченная связь между компьютерами сдерживала влияние цифровых технологий на экономику. Именно с появлением недорогой, коммерческой, межкомпьютерной связи (Интернета) предоставление информации стало оказывать ощутимое влияние на рынки [173]. С 1990 по 1995 год Интернет быстро распространился, и ключевую роль в этом процессе сыграли образовательные институты [174]. Со временем новые технологии были размещены поверх базового Интернета на основе TCP/IP, включая браузеры, поисковые системы, онлайн-магазины, социальные сети и многие другие.

Ватанабе, Тоу, Неиттаантаки проанализировали развитие ключевых ИТ в их взаимосвязи, влиянии на цифровизацию экономики и поэтапной эволюции в 1970–2020 годах (рис. 1.3).

Анде, Адебиси, Хаммоудех, Салеем проследили эволюцию развития IT в экономике в разрезе внедрения технологий IoT с 1830 по 2018 год [175], выделив в качестве целевых технологий – признание технологий IoT со стороны ЕС; использование IoT для энергосистем, самоуправляемых автомобилей; разработку глобальных стандартов IoT; интеграцию AI, ML, Блокчейн в IoT.

В разрезе финансового сектора экономики ИТ оказали существенное влияние на развитие данной отрасли, сделав возможным беспрецедентный рост цифровых транзакций и диверсификации продуктов. Выделяют пять основных технологических инноваций, повлиявших на развитие финансового сектора [176]:

1) компьютеризированные информационные системы в 1950-х годах;

2) банкоматы в 1960-х годах;

3) электронная торговля акциями в 1970-х годах;

4) мэйнфрейм-компьютеры в 1980-х годах;

5) Интернет в 1990-х – начале 2000-х годов.

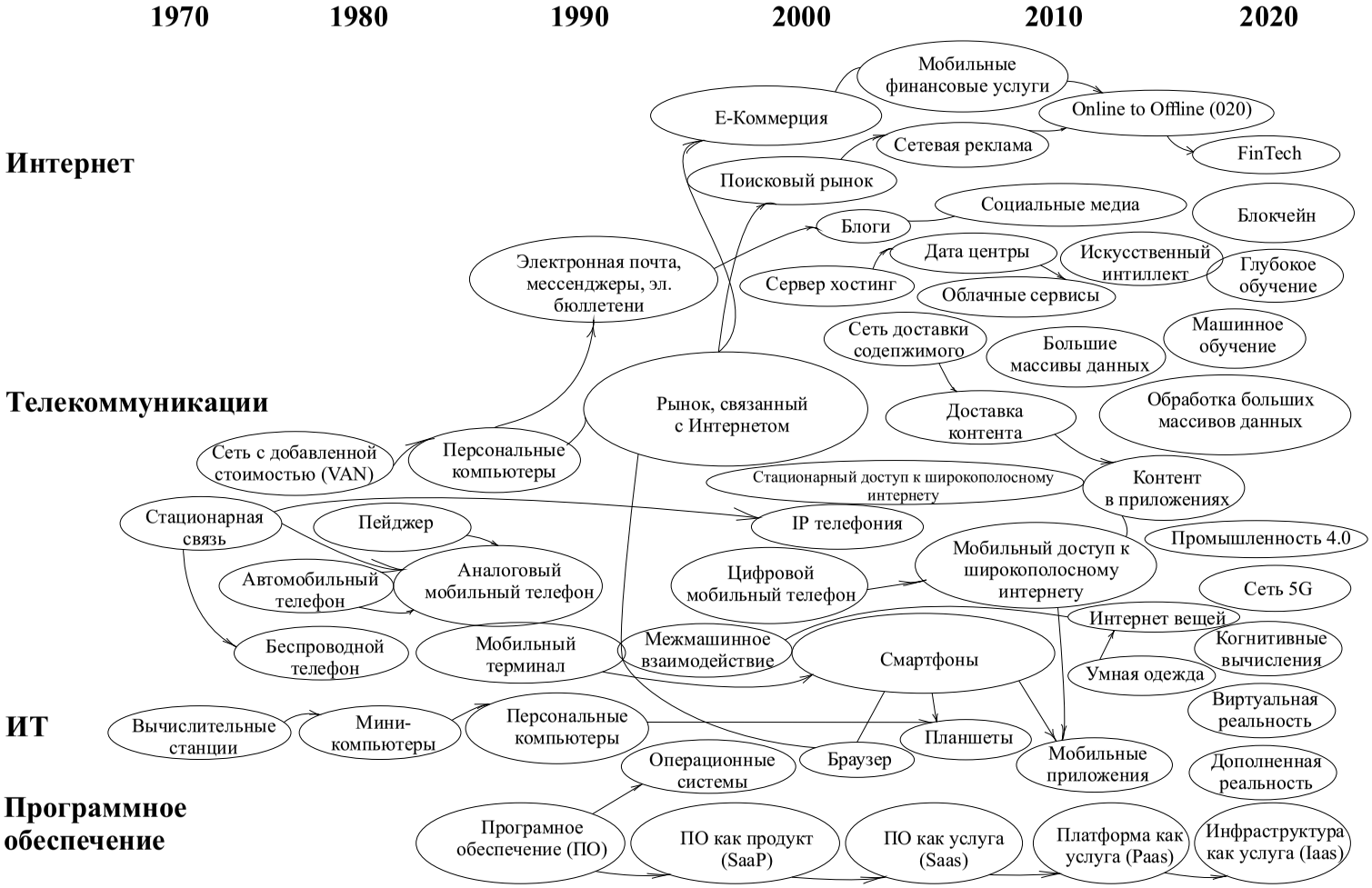


Рис. 1.3. Технологическая эволюции во взаимосвязи развития Интернета, телекоммуникаций, ИТ и программного обеспечения [157]

Мегаргел, Шанкарараман, Редди выделили следующие этапы эволюции банковских IT-систем: «эра обработки данных» (транзакция была единственным цифровым взаимодействием с клиентом), «эра клиент-сервер» (большое количество пользователей получили доступ к своим бизнес-системам в режиме 24/7) и «эра прогнозирования» (решения принимаются на основе данных, которые могут быть транзакциями или бизнес-событиями, оцениваются как в реальном времени, так и в базах данных) [177].

Дула, Ли, Чуен [178] выделяют шесть этапов развития цифровизации финансового сектора в разрезе внедрения новых платежных технологий. Вонглимпиярат [12] выводит эволюцию технологий в платежных системах с 1600-х годов – периода появления «общества, основанного на наличных финансовых средствах», характеризуемого формированием банковской системы, созданием чековой клиринговой системы и заканчивает 2016 годом – формированием «безналичного общества». Анализ показывает неравномерное ускорение внедрения цифровых технологий в финансовом секторе: 1-й этап охватывает 100 лет, 2-й – 250 лет, 3-й – 20 лет, 4–6-й – 10 лет, 7-й – 16 лет.

Таким образом, проведенный анализ показывает, что формирование цифровой экономики происходило поэтапно и связано с появлением, внедрением, распространением и коммерциализацией технологий. Этапом зарождения цифровизации следует считать создание вычислительной машины с программным кодом для расшифровки кодифицированных сообщений в период Второй мировой войны (40-х годах XX века). Профильное распространение цифровых технологий на начальном этапе осуществлялось, главным образом, в банковской сфере для ускорения платежных и расчетных транзакций и снижения издержек их обработки (60–70-е годы XX века). Широкое распространение цифровых технологий обусловлено разработкой и стремительным удешевлением электронно-вычислительных систем, которые из мейнфрейм компьютеров преобразовались в персональные вычислительные машины, доступные не только для широкого круга пользователей – юридических лиц, но и обычных граждан со средним уровнем дохода (70–80-е годы XX века). Фазовый переход к новому качеству использования цифровых технологий для коммуникаций произошел с открытием доступа к глобальной сети Интернет (80–90-е годы XX века). Именно внедрение возможностей удаленного взаимодействия через глобальную информационную сеть создало предпосылки для начала

развития цифровой экономики в форме E-commerce в конце 90-х годов XX – начале XXI века. Важным импульсом для формирования цифровых платформ и их экосреды стали социальные сети (с 2005 года). Распространение и коммерциализация цифровых финансовых инструментов, которые легли в основу новых бизнес-моделей и направлений цифровизации, можно датировать 2010 годом (состоялась первая товарообменная операция «цифровые активы» – «реальный товар»).

Базовой единицей (BU) системы цифровой экономики является сущность, представляющая собой амбивалентность программного (цифрового) продукта (кода) и цифровых данных (информации / знаний). Основоположником формирования современной концепции цифровых вычислительных машин [179] является Тюринг, который в 1936 года доказал возможность использования универсальных вычислительных машин для решения различных задач[1]. В 1948 году создан первый электронный компьютер с хранимой в памяти программой. Стандартизация подходов к понятию цифровой единицы информации связана с введением понятия «бита» (byte), предложенного в 1956 году Бухгольцем при разработке компьютера IBM Stretch. Таким образом, к 1956 году конвергенция новых подходов к разработке программного обеспечения и выработка стандарта хранения цифровых данных для последующей обработки вычислительными машинами сформировала основу для поступательного внедрения цифрового технологического уклада в экономическую систему. Именно цифровые данные являются драйвером развития современной экономики, формирующим в качестве инструмента новый характер производственных отношений, оптимизируют принятие стратегических и операционных решений на основе использования потенциала BDA. Сетевая инфраструктура позволяет подключать цифровые устройства для сбора и передачи цифровых данных в режиме реального времени. Цифровые данные передаются (обмениваются) с использованием специализированных платформ. Барьеры для обмена и объединения данных значительно снижаются, объединяя различные источники данных таким образом, что генерируемая ценность намного превышает сумму ее частей. Ускоряется разработка на основе AI/ML новых возможностей обнаружения взаимосвязей данных для стимулирования инноваций. Цифровые данные

[1] «On Computable Numbers, with an Application to the Entscheidungsproblem» (1936 год)

становятся продуктом, основным (дополнительным) источником доходов компаний, а качество цифровых активов предприятий определяет уровень их конкурентоспособности. В этой связи важнейшим элементом управления на макро- и микроуровнях становится обеспечение конфиденциальности, целостности и безопасности цифровых данных.

При рассмотрении эволюции развития цифровой экономики как системы представляется целесообразным выделить следующие стадии ее становления (рис. 1.4).

Рис. 1.4. Стадии становления цифровой экономики (разработано автором)

Базовой является стадия зарождения цифровой экономики, сопряженная с конвергенцией программного обеспечения и цифровых данных, созданием, соответственно, базовой единицы системы цифровой экономики (BU), и поступательным профильным внедрением электронных средств обработки данных, в первую очередь, в банковской сфере, а также формированием сегмента электронной торговли для осуществления транзакций в формате P2P и P2B.

Стадия возникновения цифровой экономики обусловлена формированием замкнутого контура системы сплошной цифровизации (комплексной цифровой экосистемы) на уровне отдельных отраслей и сфер деятельности, связана с платформизацией экономических отношений, конвергенцией комплексных технологических и экономических решений на уровне реализации концепций: Smart City, Intellectual Transport Systems, Industry 4.0, Agriculture 4.0, Smart Supply Chain, Smart Grid, E-Commerce», Telemedicine, FinTech, CBDC, RTGS, E-Government и прочие. Традиционные отрасли экономики

доминируют, но поступательно теряют долю в ВВП. BU становится одним из основных драйверов экономического роста, повышения эффективности производства и конкурентоспособности предприятий и продуктов (товаров, работ, услуг). Формируется рынок BU. Размер цифровой экономики (для экономики секторов, подверженных цифровизации) должен достичь 50% мирового ВВП[2]. По прогнозам компаний LETA Capital и Devar, цифровые технологии достигнут не менее 50% мирового ВВП в течение следующих 15–25 лет [179].

Для стадии становления цифровой экономики характерно формирование BU множества узкоспециализированных рынков систематизированной, универсальной, деперсонализированной, технологически нейтральной информации. Усиливаются требования национальных и международных регуляторов к безопасности BU. Доля экономики секторов, подверженных цифровизации, превысит 75% ВВП.

Стадия характеризуется изменением формы BU, трансформацией рынков цифровых данных с учетом новых, возможно, квантовых возможностей вычислений. Имеет место реактивная реакция экономической системы на возникающие вызовы и требования окружающего мира, замещение устаревших цифровых концептов новыми. Доля экономики секторов, подверженных цифровизации, снизится до 50% ВВП.

Исчезновение цифровой экономики станет завершающей стадией смены экономической парадигмы на новую, удовлетворяющую новым потребностям и вызовам, связанным с изменениями (в том числе технологическими) окружающего мира. Для данной стадии характерно доминирование BU новой, возможно, квантовой экономической системы. Доля экономики секторов, подверженных цифровизации, составит менее 25% ВВП.

О характере динамики развития цифровой экономики на современном этапе свидетельствует целый ряд показателей. Так, по данным ЮНКТАД, в 2017 году цифровая экономика США составляла 6,9% ВВП для экономики цифровых платформ и 21,6% ВВП для экономики секторов, подверженных цифровизации. Размер цифровой экономики КНР – 6,0% ВВП для экономики цифровых платформ и 30,0% ВВП для экономики секторов, подверженных цифровизации [160]. Оценивая цифровую экономику с точки зрения

[2] Размер мировой цифровой экономики в 2017 году, по данным ЮНКТАД, составил 4,5% ВВП (для экономики цифровых платформ) и 15,5% ВВП (для экономики секторов, подверженных цифровизации) [160].

совокупной стоимости, созданной на основе цифровых товаров, услуг и цифровизации традиционных отраслей, следует отметить, что в ЕС ИКТ-компании растут ежегодно на 14%, телекоммуникационные компании на 3%, в то время как другие транснациональные корпорации растут только в среднем на 0,2% [180]. Глобальная занятость в секторе ИКТ увеличилась с 34 млн человек в 2010 году до 39 млн человек в 2015 году, при этом наибольшая доля занятых приходится на сектор компьютерных услуг (38%) [160]. В 2018 году экспорт услуг с цифровой доставкой составил 2,9 трлн долларов, или 50% мирового экспорта услуг. В 2020 году в результате пандемии отмечен резкий рост электронной коммерции. В Китае доля электронной коммерции в розничной торговле выросла с 22% до 27% в 2020. В Индии наблюдался 2%-й рост, в Соединенных Штатах он составил 5% в год [181].

По состоянию на 2018 год пять самых дорогих брендов – это компании, занимающиеся цифровыми технологиями: Apple, Google, Microsoft, Facebook и Amazon. В начале января 2021 г. пять крупнейших мировых технологических компаний составляли 23% идекса S&P 500 по рыночной капитализации, что на 4,6% больше, чем в конце января 2020 года [182]. Согласно прогнозам WEF, по окончании пандемии COVID крупные технологические игроки выйдут с более сильными и разнообразными потоками доходов и большей инвестиционной силой. При этом барьеры для входа на цифровой рынок будут расти еще более быстрыми темпами, так как объем вычислительной мощности ведущей системы искусственного интеллекта удваивался каждые два месяца. Восстановление также придаст новый импульс приобретению стартапов крупными технологическими компаниями, а также их экспансии в другие сектора, такие как розничная торговля, здравоохранение, транспорт и логистика.

Таким образом, следует отметить высокую динамику увеличения доли цифровой части в мировой экономике как в целом, так и на уровне ведущих государств, что обусловлено более интенсивным ростом компаний ИКТ сектора, а также их значительной капитализацией.

Ожидается, что доходы от цифровизации для игроков ИКТ будут расти на 13,3% ежегодно – с 939 млн долларов США в год [183] (в 2016 году) до 3,2 млрд. долларов (в 2026 году). При этом доходы от внедрения 5G для компаний сектора ИКТ составят 1,2 млрд долларов. Рынок мобильных операторов в 2026 году достигнет 193 млрд долларов США для владельцев сети, 507 млрд долларов США для поставщиков услуг и 582 млрд долларов США для создателей сервисов [184].

Цацис, Карноускос, Хёллер, Бойл, Муллиган [185] в качестве основных изменений в мировой экономике, технологических и научных тенденций, выделяют следующие.

1. Мировая экономика находится в состоянии перехода от постиндустриальной эры к цифровой экономике, от товарно-ориентированной экономики к сервисно-ориентированной. Это подразумевает пожизненную ответственность за продукт, используемый в предложении услуг, и во многих случаях требуется, чтобы продукты были подключены и содержали встроенные технологии для сбора данных и информации.

2. Ограниченность природных ресурсов, экономное и более эффективное использование в условиях растущего населения планеты и связанных с этим потребностей в экономическом росте налагают все больше ограничений на использование ресурсов, внедрение концепции экономики замкнутого цикла, или циркулярной экономики.

3. Рост благосостояния приводит к сдвигу в демографических структурах по всему миру, наблюдается старение населения, что предопределяет необходимость увеличения социальных расходов.

4. Рост глобального среднего класса приводит к увеличению ожиданий в отношении благополучия и корпоративной социальной ответственности, чему все в большей степени будут способствовать технологии.

5. Общественная и национальная безопасность становятся все более актуальными по мере того, как общество становится все более развитым и более уязвимым. Это связано как с уменьшением смертности и улучшением состояния здоровья, так и с предупреждением роста преступности.

6. Резкий рост городского населения создает совершенно новый уровень требований к городской инфраструктуре.

Важно отметить роль технологий в становлении цифровой экономики на современном этапе. Принимая во внимание четырехфакторную модель экономической системы, включающую такие элементы, как производство, перераспределение, обмен и потребление, представляется целесообразным исследовать влияние современных технологий на их трансформацию.

Как показано в табл. 1.6, ключевыми цифровыми технологиями, определяющими направления развития современной экономики, являются: 5G телекоммуникации, облачные вычисления, IoT, Блокчейн, Биткойн, смарт-контракты, AI, аналитика Big Data, платформизация.

Таблица 1.6

Четырехфакторная модель экономической системы в разрезе современных цифровых технологий (разработано автором)

Современные цифровые технологии	Экономические факторы			
	производство	распределение	обмен	потребление
5G телекоммуникации	Предоставление высокотехнологических услуг, в том числе в сфере промышленного производства в связке с технологиями IoT	–	–	Производственное потребление услуг в связке с технологиями IoT
Cloud Computing	Реализация концепции Digital Twins с переносом физических производственных процессов в виртуальную облачную среду: «киберфизический подход»	Оптимизация затрат различных предприятий за счет использования инфраструктуры аутсорсинговых облачных компаний	–	Производственное потребление услуг в связке с технологиями IoT
IoT	Реализация концепции Industry 4.0	–	–	Производственное потребление услуг в связке с технологиями облачных вычислений и 5G
Блокчейн, криптовалюты, смарт-контракты	Использование Блокчейн для реализация отдельных производственных процессов (например, управление цепочками поставок)	Распределение роялти с использованием технологий Блокчейн	Использование криптовалют для оплаты за товары, работы и услуги. Реализация встроенных механизмов смарт-контрактов для осуществления двусторонних сделок без посредников	–

Окончание табл. 1.6

Современные цифровые технологии	Экономические факторы			
	производство	распределение	обмен	потребление
AI, аналитика Big Data	Реализация концепций Industry 4.0, FinTech	–	–	Использование потенциала AI совместно с Big Data для прогнозирования уровней потребления, динамики рынков, формирования цифровых портретов клиентов
Платформизация	Использование общих производственных платформ для оптимизации производственных процессов в рамках корпораций	Использование общих платформ в рамках концепции «шеринговой экономики»	Использование торговых платформ для реализации товаров, работ и услуг как на уровне B2P, так и B2B	Формирование экосреды платформ для генерирования дополнительных доходов за счет реализации возможностей предоставления дополнительных работ, товаров и услуг

ПРООН и Международный союз электросвязи в программе Connect 2020 Agenda подчеркивают, что информационное общество ускоряет экономическое и социальное развитие в различных странах [186, 187, 188]. Такие технологии, как телекоммуникации, облачные вычисления, IoT, Big Data, расширили информационное общество за счет доступа к различным источникам и большим объемам цифровых данных, создав условия для совместной работы людей из любой точки мира и массива новых автономных цифровых устройств, подключаемых ежегодно.

Доступность Интернета стала возможной в основном благодаря беспроводным и сотовым технологиям, быстрому развертыванию сотовых сетей 3G, 4G/LTE и грядущих систем 5G в глобальном масштабе.

Эти системы обеспечивают повсеместное и относительно дешевое подключение с подходящими характеристиками для многих приложений, включая низкую задержку и способность обрабатывать большие объемы данных с высокой надежностью. Мобильные сети 5G подразумевают подключение большого количества пользовательского оборудования, поддержку связи между машинами (M2M), обеспечение быстрого времени отклика и увеличение скорости передачи данных в 1000 раз [189, 190]. Названные технологии являются базой для развертывания комплексных технологических решений (метатехнологий) Industry 4.0, Smart City, Smart Grid и пр. По оценкам McKinsey, общие доходы от модулей 5G IoT в сфере B2B увеличатся с примерно 180 млн долларов в 2022 году до почти 10 млрд долларов к 2030 году [191].

Развертывание инфраструктуры мобильной сети 5-го поколения (5G) является важной частью стратегии «Цифровой повестки для Европы», в рамках которой к 2025 году планируется обеспечить непрерывное покрытие 5G для всех городских районов и основных наземных транспортных путей [192]. 5G, поддерживающая новые инновационные приложения, требующие низкой задержки и высокой скорости передачи данных, произведет революцию в сфере коммуникаций [193]. Расширятся производительные возможности сети и ее функциональность: от простого подключения людей к подключению машин и устройств. Это обеспечит эффективное соединение между интеллектуальными устройствами и приложениями, взрывной рост трафика данных мобильных пользователей

в широком спектре новых инновационных услуг для различных сред[3].

Данная технология является важнейшим технологическим драйвером «отраслевой цифровизации», так как специальные характеристики технологий 5G, а именно низкая задержка, высокая емкость данных и высокая надежность, могут использоваться для оптимизации существующих промышленных процессов, а также реализовывать новые [194]. Прогнозируется создание новых возможностей для бизнеса в таких отраслях, как промышленное производство, общественная безопасность, производство и распределение энергии, автомобилестроение, транспорт и здравоохранение. Это может означать использование высокой надежности или низкой задержки 5G для разработки более гибких и надежных отраслевых коммуникационных решений, например для управления роботами в реальном времени в различных отраслях промышленного производства и других системах. По прогнозам компании Ericsson, к 2026 году количество абонентов 5G достигнет 3,5 млрд человек [195]. В 2021 году крупнейшие сотовые операторы США – AT&T и Verizon выкупили у государства права на использование частот 5G на 80 млрд долларов; развертывание сети начато в 2022 году[4].

Облачные вычисления (cloud computing) также являются новой тенденцией и находят серьезное применение как в государственном, так и в частном секторе [122]. Как отмечает ряд исследователей, для современного уровня развития данной технологии характерен переход от облачных вычислений как продукта к вычислению как услуге, предоставляемой потребителям через Интернет [196]. Определение облачных вычислений, в основном используемое в экономической литературе, базируется на формулировке Национального института стандартов и технологий США (NIST), который

---

[3] Современная мобильная индустрия включает в себя: 1) специализированные компании, занимающиеся технологиями и компонентами; 2) разработчиков стандартного инфраструктурного оборудования; 3) поставщиков сетевых услуг; 4) последующую реализацию мобильных устройств, соответствующих стандартам; 5) поставщиков программного обеспечения; 6) провайдеров контента, от частных лиц до конгломератов СМИ. Многие компании охватывают два или более из этих звеньев в цепочке создания стоимости [60].

[4] Авиакомпании отменяют рейсы из-за запуска 5G. Правда, это все касается только спора американских сотовых компаний с американскими же перевозчиками. – Режим доступа: https://meduza.io/feature/2022/01/21/aviakompanii-otmenyayut-reysy-iz-za-zapuska-5g-pravda-eto-vse-kasaetsya-tolko-spora-amerikanskih-sotovyh-kompaniy-s-amerikanskimi-zhe-perevozchikami?utm_source=telegram&utm_medium=live&utm_campaign=live. – Дата доступа: 21.01.2022.

характеризует их как «модель для обеспечения повсеместного, удобного сетевого доступа по требованию к общему пулу настраиваемых вычислительных ресурсов (например, сетей, серверов, хранилищ, приложений и услуг), которые могут быть быстро предоставлены и выпущены с минимальными усилиями или услугами управления при взаимодействии с провайдером» [197]. Согласно эталонной архитектуре облачных вычислений NIST, определены пять основных действующих лиц: потребитель облачных услуг, поставщик облачных услуг, аудитор облачных вычислений, оператор облачных вычислений и брокер облачных вычислений. Модели развертывания облачных вычислений подразделяются на четыре типа: публичные, частные, гибридные и сообщества. Среди основных моделей облачных услуг выделяют: инфраструктуру как услугу (IaaS), платформу как услугу (PaaS) и программное обеспечение как услугу (SaaS)[5] [198].

Среди основных преимуществ облачных вычислений выделяют: экономичность, практически неограниченное хранилище цифровых данных, резервное копирование и восстановление информации, автоматическая интеграция программного обеспечения, легкий доступ к информации, быстрое развертывание, гибкость, более простое масштабирование услуг и предоставление новых услуг. Основными недостатками облачных вычислений являются: технические проблемы, законодательные лакуны, безопасность размещенных в облаке данных, подверженность данных к кибератакам, относительно высокая стоимость размещения, негибкость и отсутствие технической поддержки в режиме 24/7 [122].

В экономическом контексте сервисы облачных вычислений представляют собой новую бизнес-модель, которая обеспечивает пользователям доступ к сервисам в любое время [199]. Облачные вычисления становятся все более конкурентоспособными благодаря предоставлению клиентам с большей гибкостью распределения ресурсов и относительно более низкой стоимостью владения.

[5] Кроме того, разрабатываются новые модели услуг, такие как «Хранилище как услуга» (Storage as a service STaaS), «Безопасность и защита данных как услуга» (Security and data protection as a service SDPaaS) и «Центр безопасности операций как услуга» (Security operations center as a service SOCaaS). Облачная система способна поддерживать большой ресурс в соответствии с конкретными, личными и детальными требованиями, используя «Мониторинг как сервис» (MaaS), «Данные как сервис» (DaaS), «Связь как сервис» (CaaS), «Безопасность как сервис» (SecaaS), «Маршрутизация как услуга» (RaaS). «Все как услуга» (AaaS) – это собирательный термин, который объединяет несколько понятий «X как услуга» [201, 202, 203].

С экономической точки зрения представляется существенным тот факт, что облачные технологии позволяют заменить капитальные расходы с фиксированной стоимостью для организаций-пользователей (для создания центра обработки данных) – на операционные расходы с переменной стоимостью (покупка услуг в центре обработки данных) [200]. Организация может приобрести практически любое количество облачных сервисов, поэтому даже небольшие компании могут начать с минимального уровня и получать оплату в зависимости от объема использования. Облачные вычисления являются более экономичными по сравнению с использованием собственного центра обработки данных, поскольку вычислительные ресурсы можно приобретать по мере необходимости. Ожидается, что в 2021 году доход от облачных сервисов достигнет 300 млрд долларов [204]. Оценки, основанные на данных компаний ЕС, свидетельствуют, что увеличение доли фирм, использующих облачные вычисления на 10% в отрасли, приводит через три года к увеличению производительности на 2,3% для средней компании отрасли [205].

Важно отметить, что облачные вычисления следуют централизованной схеме, согласно которой вычисления и хранилище развертываются в удаленном центре обработки данных [206]. Однако данный подход сталкивается со значительными ограничениями при работе с этими новыми технологиями, которые требуют реакции в реальном времени и низкой задержки отклика. В связи с этим в качестве средства улучшения возможностей облачных вычислений предложена концепция «пограничных вычислений» (Edge Computing) [207, 208, 209]. Пограничные вычисления – это усовершенствованная версия облачных вычислений, которая сокращает время ожидания, уменьшая время отклика сервисных служб для конечных пользователей. Пограничные вычисления минимизируют нагрузку на облако, предоставляя ресурсы и услуги в пограничной сети, обеспечивая такие преимущества, как экономия пропускной способности и ресурсов хранения, низкая задержка отклика, увеличенная масштабируемость, повышение изоляции и конфиденциальности сети [210].

Указанная технология находит свое применение в таких секторах, как розничная торговля, промышленность, энергетика, биотехнологии, фармацевтика, химия или электроника, где данные из физического оборудования или устройств генерируются и могут быть объединены с бизнес-данными, такими как инвентаризация, производство и планирование технического обслуживания.

Концепция «туманных вычислений» (Fog Computing), разработанная компанией Cisco [211, 212], позволяет приложениям работать непосредственно на границе сети через интеллектуальные подключенные устройства. Туманные вычисления представляют собой расширение парадигмы облачных вычислений, которая переносит ресурсы и услуги из базовой сети в пограничную сеть. Это виртуализированная платформа, предоставляющая услуги хранения и вычисления в пограничной сети. Концепция туманных вычислений является самой современной с точки зрения современной оцифровки в обрабатывающей промышленности [213]. Среди преимуществ туманных вычислений выделяют возможность настройки пользователем уровня безопасности, а также низкую задержку связи.

Следует отметить отсутствие четкого различия между туманными и пограничными вычислениями, поскольку как интеллектуальные, так и вычислительные возможности вытесняют централизованную инфраструктуру в логические пределы сети вблизи источников данных и пользователей [214]. Но с точки зрения управления ресурсами, туманные вычисления, по сравнению с пограничными, являются высоковиртуализированной платформой, которая предоставляет вычислительные, сетевые сервисы между конечными устройствами и центрами обработки данных облачных вычислений[6] [215, 216].

Важным направлением цифровизации экономики является внедрение IoT. Существует множество различных технических и стратегических определений IoT (Интернета вещей). Счетной палатой США в 2017 году представлено определение IoT как «набора устройств, адресуемых по интернет-протоколу, которые взаимодействуют с физической средой и обычно содержат элементы для зондирования, обмена данными, обработки и приведения в действие» [217]. Технологии IoT, встроенные в сложные системы, обладают неотъемлемыми возможностями не только сбора данных, их обмена и обработки, но и перемещения или управления компонентом или системой автономно, потенциально без участия человека [218].

Вместе с тем следует отметить, что IoT – это не единая технология, а комбинация нескольких технологий, которые включают в

[6] В большинстве сценариев туманные вычисления часто используются, когда задача ориентирована на обслуживание, тогда как пограничные вычисления происходят чаще, если это аналитическая задача [216].

себя коммуникационные, информационные технологии, электронные датчики и исполнительные механизмы, а также последние достижения в области вычислительной техники и аналитики [219].

Исследования показали, что из-за высокой стоимости развертывания целесообразно использовать технологии IoT-сетей в критических и важных случаях [220]. В экономической литературе выделяют следующие сектора-реципиенты и области применения технологий IoT: промышленная автоматизация, транспорт и логистика, энергетика, сельское хозяйство, здравоохранение, городская инфраструктура, национальная безопасность, охрана окружающей среды [221].

Наличие интеллектуальных систем мониторинга, счетчиков в контексте интеллектуальных экосистем (например, Smart Grid), позволяет потребителям и поставщикам электроэнергии динамически анализировать ее потребление и затраты, стимулируя таким образом повышение энергоэффективности и снижение затрат [222, 223]. Так, экспериментальная установка в 2012 году датчиков IoT в пяти офисных зданиях для сбора данных, связанных с использованием энергии и эксплуатационной эффективностью, привела, по оценкам Управления общих служб США (GSA), к 15 млн долларов годовой экономии [224]. Ожидается, что приложения здравоохранения и связанные с ними услуги IoT, такие как мобильное здравоохранение и Telemedicine, обеспечивающие медицинское обслуживание, профилактику, диагностику, лечение и мониторинг, как ожидается, к 2025 году обеспечат ежегодный рост мировой экономики на 1,1–2,5 трлн долларов в год [225, 226].

Органы национальной обороны и безопасности США с 2011 года проводят эксперименты с технологиями IoT как в направлении изучения их кибербезопасности, так и эффективности использования в боевых условиях. Так, Министерство обороны США отслеживает логистику поставок товаров военного или двойного назначения в 3,5 млрд транзакций в месяц, генерируемых 67 логистическими системами Минобороны и 250 коммерческими перевозчиками. Транспортное командование Министерства обороны США установило мониторинговые датчики для обнаружения военных контейнеров, призванные предупреждать военный персонал о любых несанкционированных вторжениях с помощью системы спутникового наблюдения [224].

Таким образом, внедрение IoT в экономическом контексте направлено, в первую очередь, на повышение операционной эффективности организаций и отраслей путем снижения затрат, повышения производительности и более эффективного использования дорогостоящего оборудования [185]. IoT воздействуют на пять основных отраслевых факторов, а именно: проектирование и инновации, использование активов и планирование доходов, цепочки поставок и проектирование логистики, повышение производительности ресурсов и расширение опыта заинтересованных сторон [227].

Внедрение IoT в операциях и цепочках поставок дает ощутимые коммерческие преимущества, в том числе улучшенные операционные процессы, низкие риск и затраты. Дополнительные преимущества включают в себя прозрачность, адаптацию, гибкость и виртуализацию в цепочках поставок [228, 229]. IoT предоставляет новые возможности с точки зрения управления и контроля. Данные, выпущенные из системы IoT, предоставляют лицам, принимающим решения, новое понимание ценностного предложения, создания ценности, помогая им укрепить свои связи с клиентами и принять более эффективную политику и практику [230].

Прогнозируется, что в следующем десятилетии IoT окажет огромное влияние на глобальную экономическую платформу [231]. Ряд исследователей указывают, что трансформация и оптимизация глобальной экономики будут зависеть исключительно от масштаба внедрения IoT-устройств, доступности и долговечности интеллектуальных устройств и шкалы приемлемости технологий как для потребителей, так и для работников [232]. По мере расширения внедрения данных технологий, согласно прогнозам экономистов, экономика будет носить полностью автономный и цифровой характер – все участники и рынки подключены к сети, а также подключены и автоматизированы бизнес-процессы, продукты и услуги, которые могут быть полностью и гибко адаптированы и собраны для индивидуальных нужд.

При этом важно также отметить эволюцию самой парадигмы IoT в контексте инноваций и технологий. Исследователи отмечают сдвиг от подхода IoT, ориентированного, на устройства, к интеллектуальной инфраструктуре IoT.

Цацис, Карноускос, Хёллер, Бойл, Муллиган отмечают, что использование IoT-решений в экономике и социальной сфере будет поступательно возрастать по следующим причинам [185].

1. Повышенная потребность в понимании физической среды в ее различных формах – от промышленных установок до общественных мест и ожиданий потребителей. Эти требования часто обусловлены повышением эффективности, достижением целей устойчивости или улучшением здоровья и безопасности.

2. Доступность технологий и услуг для более дешевого сбора и анализа данных с помощью улучшенных сетевых и аналитических инструментов.

3. Снижение затрат на компоненты для устройств IoT, которые снабжают повседневные объекты сенсорными и вычислительными возможностями.

Таким образом, IoT-рынок будет становиться все более привлекательным с экономической точки зрения по причине а) зрелости технологий; б) снижения затрат; в) роста потребностей предприятий и общества.

По оценкам компании Intel, в 2006 году в мире использовались около 2 млрд устройств [221, 233]. Производитель ИТ-оборудования Juniper прогнозирует, что к 2022 году число подключенных IoT-устройств, датчиков и оборудования достигнет более 46 млрд [185]. Statista прогнозирует 75,44 млрд подключенных устройств к 2025 году [234]. Глобальный рынок IoT к 2023 году достигнет 724,2 млрд долларов [235]. Предполагается, что IoT обеспечит средний экономический приток в размере 7,5 трлн долларов в год к 2025 году во всех цепочках поставок [236]. Ожидается, что к 2022 году потоки цифровых данных M2M составят до 45% всего трафика Интернета [237]. По прогнозам ЕС, к 2025 году количество подключенных устройств составит до 25 млрд единиц, из которых 25% будут находиться в Европе [238]. В соответствии с исследованием McKinsey, экономическая ценность IoT-решений в 2020 году составила в 1,6 трлн долларов. К 2030 году IoT сможет обеспечить глобальную стоимость от 5,5 до 12,6 трлн долларов. При этом имплементация IoT-технологий в производстве будет генерировать наибольшую потенциальную экономическую ценность – около 26%, на втором месте – здоровье человека (10–14%). Ключевую роль в имплементации технологии будет играть КНР, чья доля достигнет к 2030 году 26% мирового рынка IoT (в 2020 году – 22%). Доля развитых государств будет поступательно снижаться и достигнет к 2030 году 55% (в 2020 году – 61%) [239].

В целом, по оценкам Морено, Замора, Скармета, к 2025 году потенциальный рынок домашней автоматизации вырастет до 44 млрд долларов [240, 241].

Вместе с тем следует выделить ряд ограничений, связанных с особенностью централизованной архитектуры IoT, включая [242]:

1) масштабируемость. Система IoT основана на управлении и контроле всех процессов с использованием центрального органа. Данная структура может масштабироваться только для небольших сетей. Развертывание централизованной системы для крупных бизнес-организаций со многими филиалами в разных географических локациях будет малоэффективным из-за сложности обработки неструктурированных данных, скорости и объема передачи информации с удаленных датчиков в единый центр;

2) стоимость. Все вычислительные операции системы IoT выполняются через центральный сервер, в этой связи предполагается, что аппаратные и программные возможности являются высокопроизводительными для того, чтобы обслуживать все узлы в сети. Существует значительный объем коммуникаций между узлами и централизованным сервером, требующих обработки и высокой вычислительной мощности для обслуживания нескольких узлов одновременно. Кроме того, нужно поддержание больших хранилищ данных. Таким образом, для системы IoT характерны большие затраты, связанные с развертыванием и обслуживанием централизованных серверов, которые увеличиваются с ростом количества устройств IoT в сети. Многие экономисты отмечают, что развертывание систем IoT – это не столько вопрос капитальных расходов (CAPEX), сколько вопрос о значительных операционных расходах (OPEX) [185];

3) конфиденциальность. Централизованная система уязвима для манипулирования данными. Сбор данных в реальном времени с различных устройств и хранение их в одном месте с полномочиями централизованного сервера делает их содержание потенциально уязвимым, остается возможность нарушения конфиденциальности;

4) безопасность. Особенности централизованной системы IoT, связанные с хранением цифровых данных в одном месте, и выполнение всех операций через центральный сервер делает «Интернет вещей» уязвимой целью для различных типов атак, особенно на отказ в обслуживании (DoS) и распределенный отказ в обслуживании (DDoS). По прогнозам Международной корпорации данных (IDC),

почти 90% организаций, внедряющих IoT, в ближайшем будущем пострадают от нарушения внутренней ИТ системы на основе IoT [243, 244];

5) отказоустойчивость. В условиях централизованной системы IoT сервер выполняет все операции обработки и контролирует все узлы, подключенные к нему в сети. Это создает единую точку отказа, при которой выход сервера из строя приводит к недоступности всей системы.

Одним из вариантов преодоления недостатков эталонной архитектуры IoT является применение структуры Блокчейн, которая обеспечивает автономную, распределенную, децентрализованную и бездоверительную среду [242]. В отличие от централизованной архитектуры, Блокчейн использует децентрализованный и распределенный регистр для обработки всех участвующих узлов в сети Блокчейн, которые обеспечивают большую эффективность. Кроме того, отсутствие центрального органа повышает удобство ведения бизнеса и гарантирует надежный рабочий процесс. Децентрализованный характер основанных на Блокчейн систем IoT устранит некоторые проблемы централизованной архитектуры, такие как централизованная точка отказа [245, 246]. Это также предотвратит ситуации, в которых немногие управляющие компании имеют полномочия и контролируют хранение и обработку данных значительного количества людей. Информация о транзакциях приложений IoT остается защищенной, поскольку все транзакции защищены криптографическим шифрованием [247]. Блокчейн обеспечивает высокий уровень прозрачности, обмениваясь деталями транзакции между всеми узлами-участниками, вовлеченными в эти транзакции. Интеграция IoT и Блокчейн может предоставить новый путь для автоматизированных систем обслуживания и бизнес-моделей [241].

Информация IoT в Блокчейн может оставаться неизменной, участники системы способны проверять подлинность данных, сохраняя уверенность, что они не были подделаны [247]. Кроме того, технология обеспечивает отслеживание и учет цифровых данных датчиков. Надежность является ключевым аспектом Блокчейн для внедрения IoT. Более того, существует возможность в рамках Блокчейн рассматривать обмен сообщениями устройств как транзакции, подтвержденные смарт-контрактами, и обеспечивать безопасность

обмена данными между устройствами[7]. Текущие безопасные стандартные протоколы, используемые в IoT, могут быть оптимизированы с помощью Блокчейн [248].

По мнению Такора, Вагашия, Пателя, Доши, интеграция IoT и технологии Блокчейн приведут к созданию новых бизнес-моделей стоимости, оптимизации экосистемы, снижению рисков, высвобождению капитала, снижению операционных издержек, ускорению обработки, обеспечению безопасности, доверительности, проверке сертификации, целостности дизайна, борьбе с контрафактной продукцией, диагностике, удаленным услугам и пр. [247].

Альтернативой интеграции Блокчейн с IoT является интеграция IoT и облачных вычислений [249], которая позволяет преодолеть такие ограничения IoT, как обработка, хранение и доступ. Однако облачные вычисления обычно предоставляют централизованную архитектуру, которая, в отличие от Блокчейн, усложняет надежный обмен для многих участников. Интеграция между Блокчейн и IoT предназначена для устранения предыдущих ограничений в дополнение к поддержанию надежных данных. Туманные вычисления направлены на то, чтобы перераспределить и приблизить вычисления к конечным устройствам, следуя распределенному подходу. Это может включать в себя более мощные устройства, чем IoT, такие как шлюзы и пограничные узлы, которые затем могут быть повторно использованы в качестве компонентов Блокчейн. Поэтому туманные вычисления могут облегчить интеграцию IoT с Блокчейн.

Блокчейн является новым и перспективным подходом для крупномасштабных и конфиденциальных распределенных IoT-систем, которые могут значительно выиграть от технологии Блокчейн, когда используются ключевые операции, такие как отслеживание объектов, управление идентификацией и политиками, отслеживание транзакций и подотчетность, координация и т. д. [250]. Делая такие операции более безопасными, автономными, гибкими и даже прибыльными, способствуя также масштабируемости, межфирменному сотрудничеству, взаимодействию, технология Блокчейн может выполнять некоторые из наиболее важных требований и функций, общих для систем с несколькими агентами и IoT, такие как

[7] Блокчейн может ускорить создание IoT-экосистемы услуг и рынков данных, где микросервисы могут быть легко развернуты, а микроплатежи могут быть безопасными в бездоверительной среде. Это улучшило бы взаимосвязь IoT и доступ к данным IoT в Блокчейн.

целостность данных, конфиденциальность, аутентичность, управление большими данными и децентрализованная координация [251].

Термин «Блокчейн» первоначально применялся для описания системы распределенного хранения записей, используемой протоколом Биткойн, в настоящее время применяется для описания любых технологий распределенной бухгалтерской книги, которые основаны на особом дизайне цепочки блоков Биткойн [252]. Термин «технология распределенного реестра» (Distributed Ledger Technology, DLT), или «реплицированная, общая книга», относится к распределенной системе ведения записей, которая доступна только для добавления и защищена с помощью согласованных протоколов. Важно отметить отсутствие единого определения в отношении данной технологии. Так, в технологическом разрезе Блокчейн представляет собой структуру, в которой транзакции хранятся в цепочке блоков, по сути, являющихся связанными структурами данных, содержащими пакет действительных и проверенных транзакций[8] [253].

Ключевые свойства Блокчейн – это то, как программное средство (программа) работает для обеспечения передачи уникальных цифровых активов (например, денег, имущества, контрактов и идентификационных данных) через Интернет, не требуя сторонних посредников, таких как банки или государственные организации [254]. Представляется, что Блокчейн является передовой инновацией,

[8] Блокчейн можно считать постоянно растущим реестром, в котором хранятся записи обо всех транзакциях, произошедших в хронологическом порядке, и содержимое их является неизменным. Каждый блок состоит из неизменяемого хэша предыдущего блока, к которому он подключен. Таким образом формируется цепочка ссылок из блоков, содержащих данные, которые могут быть уникальным образом связаны с физическим активом, таким как человек или физическое свойство. Эта распределенная база данных работает на нескольких серверах (узлах) по всей сети, причем каждый узел проверяет безопасность и целостность ввода данных в блоках в этой одноранговой сети. Поскольку центральное управление отсутствует, проверка распределяется между узлами в сети цепочки блоков. Каждый блок в Блокчейн – это запись некоторых или всех недавних транзакций, которые произошли по сети. Транзакция может содержать записи значимых событий, связанных с отслеживаемым активом. Блок содержит информацию о последних транзакциях, собственном размере, а также счетчик транзакций, который отслеживает добавление экземпляра блока в цепочку блоков, заголовок блоков, сохраняющий информацию о криптографическом хэше предыдущего и текущего блоков, временную метку и «число, использованное единожды», или случайное число Nonce, которое помогает в генерации действительных хэшей для последующих блоков. Майнинг в контексте Блокчейн подразумевает механизм для достижения консенсуса по состоянию Блокчейн, чтобы обеспечить его безопасность и защиту от несанкционированного доступа [253].

обладающей большим потенциалом эффективной синергии с другими цифровыми технологиями (в первую очередь IoT), вместе с тем изначально ориентированной на кредитно-финансовую сферу, передающей при внедрении (интеграции) с другими инновациями (либо традиционными отраслями) такие дополнительные свойства, как конфиденциальность, неизменность и прозрачность хранимых и передаваемых цифровых данных. В этой связи следует выделить ряд основных функций Блокчейн [176, 255].

1. Распределенная сеть: все участники сети могут проверить транзакции. Майнеры являются ключевыми действующими лицами в этой распределенной сети, поскольку они работают над решением вычислительных проблем, которые позволяют создавать, проверять и надежно хранить транзакции.

2. Криптография: позволяет сторонам сохранять конфиденциальность информации, пересылаемой друг другу.

3. Метка времени: каждая транзакция, которая происходит в Блокчейн, имеет метку времени, которая не может быть изменена после осуществленной записи.

Как правило, выделяют три типа сетей Блокчейн: публичные, частные и консорциум (смешанный тип) [254]. Публичный Блокчейн предполагает наличие возможности для любого участника в сети Интернет присоединиться или выйти из сети Блокчейн без необходимости предоставления форм идентификации или запроса разрешения [252]. Частный Блокчейн предполагает, что все участники сети известны и заслуживают доверия; принадлежат к контролируемому сообществу. Субъектами могут быть как отдельные лица, такие как сотрудники и клиенты, так и организации (компании или отделы внутри компаний). Пользователи частной сети Блокчейн могут иметь определенные типы доступа для записи в книгу. Частный Блокчейн составляют большинство корпоративных, промышленных и государственных проектов Блокчейн. Различные другие стороны могут иметь различные частные представления данных только для чтения (например, сотрудники по соответствию и регулирующие органы). Блокчейн консорциума объединяет элементы публичного и частного Блокчейн. В Блокчейн консорциума в качестве валидаторов функционирует уполномоченная группа, видимость сети может быть ограничена валидаторами, авторизованными лицами или не иметь ограничений.

На основе особенностей типологии Блокчейн выделяют ряд слабых и сильных характеристик соответствующих разновидностей сетей (SWOT анализ), а также угрозы, связанные с определенной типологией распределенной сети. Это позволяет выбрать наиболее приемлемый тип построения Блокчейн с учетом специфики требуемого функционала, выполняемых задач и устойчивости системы к существующим угрозам.

Важным технологическим элементом протокола Блокчейн является алгоритм согласования «консенсус», который позволяет построить открытую распределенную сеть, где все стороны могут прийти к соглашению [254]. Данный механизм призван обеспечить достижение общей надежности в распределенной сети регистров, так как предполагается, что 51% пользователей осуществляют согласование контента, хранящегося в общей книге [256]. В публичном Блокчейн алгоритмы согласования «Доказательство выполнения работы» (Proof of Work (PoW)[9] и «Доказательство доли владения» (Proof of Stake (PoS)[10] являются наиболее распространенными и популярными алгоритмами консенсуса. «Делегированное доказательство доли владения» (Delegated Proof of Stake (DPoS) служит для стимулирования заинтересованных сторон и поощрения их к участию в сети путем делегирования или передачи своих монет более крупным заинтересованным сторонам [257, 258].

---

[9] Алгоритм «Доказательство выполнения работы» (Proof-of-Work (PoW) требует, чтобы все узлы в сети конкурировали за вознаграждение при добавлении блока записей в конец цепочки. Это соревнование включает в себя поиск одноразового номера путем простого использования вычислительной мощности. Это создает модель стимулирования, согласно которой выигравший узел, который добавляет блок в цепочку блоков, получает вознаграждение цифровыми токенами – Биткойнами. Для взлома сети злоумышленник вынужден не только бороться за право добавить блок, но и конкурировать за создание самой длинной цепочки. Это подрывает экономические стимулы атак, делая их финансово затратными (тип атаки – *Sybil attack*) [252].

[10] Алгоритм «Доказательство доли владения» (Proof of Stake (PoS) предполагает, что майнер или валидатор, который создает новый блок, выбирается детерминированным образом в зависимости от его денежного вклада или доли [257, 261]. Концепция данного протокола предполагает увеличение вероятности успеха узла в создании новых цифровых токенов пропорционально количеству цифровых токенов, уже принадлежащих узлу. Логическое обоснование состоит в том, что чем больше цифровых токенов принадлежит узлу, тем больше будет заинтересованность узла в защите сети. Алгоритм согласования защищает сеть без использования вычислительной мощности от атак и снижает барьер входа, устраняя преимущества, связанные с использованием специализированного оборудования [243]. Таким образом PoS – это более дешевая и экологичная распределенная форма согласованного алгоритма. Данный протокол впервые был реализован для криптовалюты Peercoin [252].

В частном Блокчейн общим алгоритмом консенсуса является «Задача Византийских генералов» (Practical Byzantine Fault Tolerance (PBFT), которая обеспечивает консенсус независимо от злонамеренного поведения со стороны некоторых участвующих узлов[11] [259]. «Доказательство прошедшего времени» (Proof of Elapsed Time (PoET) – это частный согласованный механизм цепочки блоков, которому необходимо, чтобы все участвующие узлы идентифицировали себя, прежде чем они будут участвовать в сети [260]. PoET основан на системе честной лотереи по технологии Intel Guard Guard, где каждый участник имеет равную возможность быть победителем среди всех участников сети.

Отказоустойчивый консенсусный алгоритм «Raft» следует модели «лидера-последователя», когда отдельный руководитель избирается для принятия решения об общих состояниях сети и передает изменения на узлы-последователи. Процесс выбора, основанный на случайных настройках тайм-аута, происходит, когда лидер отсутствует или не реагирует в течение заранее определенного периода времени.

Алгоритм согласования «Ripple» (RPCA) (разработан в 2014 году) является еще одним согласованным протоколом на основе токенов без использования майнинга [252]. Целью Ripple является обеспечение безопасных, мгновенных, дешевых международных финансовых транзакций любого размера безвозвратных платежей [254].

В данном контексте следует выделить некоторые из основных функций Блокчейн [257].

1. Неизменность: информация, записанная и подтвержденная в цепочке блоков, не может быть изменена или удалена из сети. Кроме того, информация не может быть добавлена произвольно.

2. Распределенная и надежная среда: в Блокчейн любой добавляемый узел может синхронизировать и проверять все содержимое Блокчейн распределенным образом без центрального контроля. Это гарантирует безопасность и предотвращает единую точку отказа, обеспечивая доверие в системе.

---

[11] В рамках данного протокола согласования все узлы соединяются друг с другом, и законные узлы достигают системного соглашения, основанного на правиле большинства. Консенсус предполагает, что количество вредоносных узлов не может быть равным или превышающим 33% всех узлов в сети. Протокол консенсуса требует, чтобы все клиенты в сети проходили аутентификацию и авторизовались для отправки транзакций валидаторам [252].

3. Конфиденциальность и анонимность: пользователь может присоединиться к сети анонимно, информация о нем не может быть известна другим пользователям. Личная информация является конфиденциальной, безопасной и анонимной.

4. Более быстрые транзакции: обработка транзакций или событий занимает от нескольких секунд до нескольких минут.

5. Надежные и точные данные: сеть Блокчейн может противостоять злонамеренным атакам и не иметь единой точки отказа.

6. Прозрачность: Блокчейн хранит сведения о каждой отдельной транзакции или событии, которое происходит в сети. Любой участник сети может просматривать транзакции.

Одной из важнейших концепций, которая помогает повысить эффективность использования Блокчейн, являются смарт-контракты[12]. Единое определение данной технологии отсутствует, вместе с тем с экономической точки зрения, по нашему мнению, ее можно трактовать как гарантированное программным обеспечением выполнение простых односложных условий[13].

В настоящее время смарт-контракты используются как удобный способ оцифровки, обмена, автоматизации и обеспечения выполнения бизнес-процессов в сети ненадежных организаций, особенно в Блокчейн консорциумов [262], без необходимости полагаться на какую-либо единственную точку доверия. Смарт-контракт имеет ряд возможностей, которые делают его привлекательным для пользователей и предприятий благодаря таким характеристикам, как неизменность, безопасность, беспрепятственное выполнение (предполагает немедленный перевод средств, без необходимости центрального органа), транспарентность для мониторинга и надзора. Таким образом, они обеспечивают надежный способ проведения транзакций, устраняя необходимость иметь доверенных посредников для заключения сделки [263, 264]. Созданы различные платформы для написания смарт-контрактов, некоторые из них предназначены специально для этой задачи, например Ethereum (https://www.ethereum.org/)[14]. Ориентированной на предприятия версией Ethereum является Кворум («Quorum»), предназначенный для

---

[12] Концепция смарт-контракта была впервые предложена Ником Сабо в 1994 году [265].

[13] Условие «ЕСЛИ» – «ТО» («IF» – «THEN»).

[14] Ethereum – глобальная децентрализованная прикладная платформа, используемая для разработки и эксплуатации интеллектуальных контрактов [252].

работы с корпоративным Блокчейн и платформой смарт-контрактов. Кворум оптимален для любого приложения, требующего высокоскоростной и высокопроизводительной обработки частных транзакций в пределах разрешенной группы известных участников (например, группы инвестиционных банков) [254].

Смарт-контракты имеют следующие преимущества по сравнению с обычными контрактами [266].

1. Снижение рисков. По причине неизменности Блокчейн смарт-контракты не могут быть произвольно изменены после их выпуска. Более того, все транзакции, которые хранятся и дублируются во всей распределенной системе Блокчейн, отслеживаются и проверяются. В результате злонамеренное поведение, такое как финансовое мошенничество, может быть в значительной степени нивелировано.

2. Сокращение административных и сервисных расходов. Цепочки блоков обеспечивают доверие всей системы с помощью распределенных механизмов консенсуса, не проходя через центрального брокера или посредника. Умные контракты, хранящиеся в Блокчейн, могут автоматически запускаться децентрализованно. Следовательно, затраты на администрирование и обслуживание благодаря вмешательству третьей стороны могут быть значительно снижены.

3. Повышение эффективности бизнес-процессов. Устранение зависимости от посредника может значительно повысить эффективность бизнес-процесса.

Вместе с тем смарт-контракты влекут за собой проблему с точки зрения неизменности, так как после регистрации в них невозможно исправить ошибку. Единственным решением является создание нового контракта для отмены операций, выполненных по первому контракту [267].

Кроме того, может не сохраняться конфиденциальность полного исполнения договора, поскольку все транзакции доступны для всех в рамках всей сети [266].

Важно отметить сложность обеспечения исполнения смарт-контрактов из-за уязвимости компьютерных программ к сбоям. Смарт-контракты уязвимы для кибератак и мошеннических схем. Так, результаты исследования Бартолетти, Карта, Симоли схем финансовых пирамид (схема Ponzi) на Etherium с июля 2015 по май 2017 года выявило 17 777 мошеннических транзакций на сумму 410 тыс. долларов США [268].

Две другие концепции часто относятся к смарт-контрактам [267]:

«DAO» – децентрализованная автономная организация, работает исключительно по правилам, зафиксированным в смарт-контрактах на Блокчейн;

«DApp» – это веб-приложения, которые взаимодействуют с экосистемами Блокчейн и предоставляют конечным пользователям аналогичные веб-сервисы, так что базовая технология инкапсулируется аналогичным пользовательским интерфейсом [269, 270]. DApp обеспечивает быстрые транзакции с умными контрактами, которые выполняются автоматически в заранее оговоренных обстоятельствах. Ethereum как платформа позволяет разработчикам легко создавать децентрализованные приложения (DApp) с помощью технологии Блокчейн [240].

Кроме Ethereum, среди наиболее популярных платформ смарт-контрактов: Hyperledger Fabric[15] [271], Corda[16] [272], Stellar [273], Rootstock [274].

«Hyperledger Fabric» (HLF) решение позволяет внедрять инновации для широкого спектра отраслевых применений, включая банковское дело, финансы, страхование, здравоохранение, IoT, цепочку поставок. Протокол HLF реализован в платформе IBM Watson IoT ™ (платформа Blockchain-as-a-Service)[17], которая позволяет устройствам IoT отправлять данные в частные регистры Блокчейн для включения в общие транзакции с записями, защищенными от несанкционированного доступа [275, 276].

R3 Corda предназначена для работы в регулируемых средах с ограниченным числом известных участников, характерных для финансового сектора. В банковских учреждениях Corda используется для работы с универсальными стандартами обмена финансовыми сообщениями, такими как ISO 20022.

Исследователи [266] среди перспективных направлений применения смарт-контрактов выделяют финансы, шеринговую эко-

---

[15] «Hyperledger Fabric» (HLF), созданый в 2016 году в качестве проекта «Linux Foundation» при участии IBM, Intel, Soramitsu и Monax, является консорциумным решением, платформой с открытым исходным кодом, использующей технологию распределенного реестра корпоративного уровня [225].

[16] R3 Corda – это платформа распределенной бухгалтерской книги для записи и обработки финансовых соглашений, разработанная компанией R3 [252].

[17] IBM, R3, Amazon и Microsoft уже несколько лет предлагают клиентам корпоративные Блокчейн-as-a-Service-решения на базе сетей Ethereum, Hyperledger и Corda (Мир блокчейна и криптовалют: неочевидные тренды-2022. Ч. I. – Режим доступа: https://ispace.news/analytics-pro/mir-blokceina-i-kriptovalyut/. – Дата доступа 28.01.2022).

номику, государственный сектор, а также системы безопасности, передачи данных в IoT.

По мнению Дэвидсона, Де Филиппи, Потца [277], распределение управления среди множества независимых участников сети делает Блокчейн «институциональной технологией», которая должна рассматриваться через призму транзакционных издержек и экономической организации [278]. Как объясняют Каталини, Ганс, Лютер, экономический эффект от внедрения технологии Блокчейн характеризуется снижением затрат на верификацию и сетевых затрат, которые являются формами операционных затрат [279, 280]. Основной эффект институциональных технологий, таких как Блокчейн, заключается в низких транзакционных издержках экономической координации и управления между сетью экономических агентов, а не во влиянии инноваций на производительность для экономического агента. Как институциональная технология, Блокчейн способствует институциональному предпринимательству новыми формами экономической координации и управления [281].

Инновационный процесс Блокчейн внедряется во многих секторах экономики, включая финансы, сельское хозяйство, торговлю и логистику, индустрию развлечений и искусства, государственные службы, страхование, здравоохранение и энергетику [282].

Ряд исследователей выделяют следующую классификацию применения технологии Блокчейн [254]: 1) денежные активы (валюта, платежи, денежные переводы, финансы, ценные бумаги и финансовые инструменты); 2) собственность (реестры земельных участков, недвижимости и автоматических прав собственности); 3) контракты (деловые соглашения, лицензирование, регистрация, завещания и доверительные отношения, партнерские соглашения и регистрации); 4) удостоверения личности (паспорта, визы, водительские права и реестры рождений). Распределенные реестры Блокчейн создают новый способ управления экономическими и информационными транзакциями с помощью безопасных сетей связи.

Вместе с тем Блокчейн не является универсальным решением для любых бизнес-процессов, его следует рассматривать только как «средство» для решения конкретных бизнес-задач[18].

[18] Например, технология Блокчейн может повысить уровень дезинтермедиации, когда поставщики могут напрямую взаимодействовать с клиентами, устраняя необходимость в сверках, эффективно отслеживая активы и обеспечивая целостность данных [284, 285].

Блокчейн может записывать экономические операции между любыми видами активов [140, 283]. Технология Блокчейн позволяет получать информацию с отметкой времени, проверять ее подлинность и хранить. Возможные направления применения технологии включают следующие [267]:

1) нотариальное заверение документов – «Factom» является ранним примером решений Блокчейн, предоставляющих совместную неизменяемую платформу для ведения записей для бизнеса;

2) аккредитация клиентов между субъектами – клиенты одного финансового учреждения могут делиться своими учетными данными с другими учреждениями («KYC Passporting»);

3) управление цепочкой поставок – Блокчейн можно применять для отслеживания происхождения товаров или сертификации интеллектуальной собственности;

4) суверенная идентичность – Блокчейн может использоваться для управления цифровыми идентификаторами. Несколько организаций занимаются данной проблематикой, в том числе Civic.io и инициатива «World Identity Network», которая была запущена в 2017 году;

5) услуги условного депонирования – деньги могут храниться на платформе и отправляться получателю только после предоставления услуги;

6) параметрическая страховка – оплата может быть согласована заранее в случае катастрофических событий;

7) распределение роялти – платежи могут быть инициированы, когда клиенты приобретают защищенную авторским правом услугу или продукт;

8) контракты IoT (Интернета вещей) – машины могут потреблять услуги между собой на открытом рынке в режиме реального времени.

Следует отметить успешную практику применения технологии Блокчейн в области электронного правительства [247] и других сферах государственного управления[19].

В исследовании Михельмана подчеркиваются преимущества использования технологий Блокчейн для снижения затрат: 1) связанных с аудитом и проверкой транзакций; 2) между сторонами по причине отсутствия дорогостоящих промежуточных продуктов [286].

---

[19] Например, для регистрации паспортов в Дубае [293], электронной идентичности в Эстонии [294], для оцифровки свидетельств о рождении в шт. Иллинойс (США) [295], в Индии для регистрации земли [296].

Поскольку Блокчейн спроектирован с неизменяемостью в качестве одной из основных характеристик, этот факт рассматривается как гарантия подлинности и доверия, что повышает безопасность и снижает вероятность мошеннических транзакций [287, 288]. Блокчейн обеспечивает мониторинг происхождения данных, а также отказоустойчивую модель безопасности [285]. Приложения Блокчейн создают повышенный уровень безопасности по сравнению с традиционными архитектурами, поскольку они игнорируют ошибочные, вредоносные или подозрительные транзакции и узлы.

Практическое применение Блокчейн было связано со значительной экономией затрат, улучшением производительности, уменьшением человеческих ошибок и устранением необходимости бумажных процедур в контексте управления цепочками поставок и финансовыми транзакциями [289, 290].

Вместе с тем в настоящее время существует небольшое количество реального внедрения технологии Блокчейн, поэтому точные расчеты являются ориентировочными показателями и, следовательно, субъективными.

Согласно результатам глобального опроса Deloitte 2020 года, 39% руководителей и специалистов-практиков в 14 странах заявили, что уже включили Блокчейн в производственные процессы в своих компаниях. Этот показатель увеличивается до 41%, если рассматривать компании с доходом более 100 млн долларов в год. При этом в США 31% респондентов заявили о наличии Блокчейн в производстве, в Китае – 59% [291]. По данным проведенного исследования Оник, Ейх, Янг, Кима, глобальные инвестиции в Блокчейн уже составили более 6 млрд долларов [292].

Британская исследовательская компания «Juniper» в своем отчете (по состоянию на 2017 год) отметила, что 57% крупных корпораций (компании с более чем 20 тыс. сотрудников) либо активно рассматривают, либо находятся в процессе развертывания Блокчейн [297]. Ожидается, что к 2022 году экономия за счет сокращения посредников (и сетей с медленными платежами) с переходом на Блокчейн может составить 15–20 млрд долларов США [298].

В исследовании Янсити и Лакхани утверждают, что Блокчейн – это не разрушительная, а фундаментальная технология, которая может породить новые экономические и социальные системы, но потребует десятилетий, чтобы повлиять на экономическую и социальную инфраструктуру [299].

Исследования Дрешера и Рабаха [300, 301] указывают на ряд генерируемых в результате внедрения Блокчейн преимуществ, включая:

1) деинтермедиацию. Это относится к сокращению потребности в посредниках или в третьих сторонах в рамках цепочки блоков;

2) безотказность. Это преимущество относится к целостности цепочки блоков, когда стороны не могут отрицать или оспаривать свои дополнения к цепочке блоков из-за целостности истории транзакций;

3) автоматизацию. Рабочий механизм Блокчейн может заменить задачи ручного труда;

4) оптимизированный процесс. В рамках Блокчейн бизнес-процессы станут более стандартизированными, прозрачными и оптимизированными, поскольку они были переработаны для перехода от традиционных технологий;

5) скорость обработки. Более широкое использование автоматизации в процессах Блокчейн по сравнению с централизованными архитектурами, вероятно, обеспечит значительные преимущества в скорости выполнения для конкретных случаев использования;

6) снижение затрат. Чистым эффектом деинтермедиации и автоматизации является снижение затрат для тех приложений, которые могут использовать преимущества технологии Блокчейн;

7) доверие. Блокчейн эффективно заменяет доверие людей проверкой и доверием к технологиям и связанным с ними протоколам. Это, вероятно, будет существенным изменением бизнеса по сравнению с существующей рабочей практикой. Доверие к целостности безопасности и обработке платежей может перерасти в товар, поскольку Блокчейн становится повсеместным, а затраты начинают падать;

8) повышение осведомленности о технологиях. Возможно, это побочное преимущество от реализации Блокчейн, но благодаря повышению осведомленности и использованию этой технологии разрабатываются новые приложения и новое понимание.

Такие исследователи, как Моин, Карим, Сафдар, Ахмед, Имран, к преимуществам Блокчейн добавили, в том числе [302]:

а) безопасность и масштабируемость. Технология Блокчейн не предполагает единой точки отказа, и кибератаки на такую систему сложны, затратны и малоэффективны для организации. Системы биткойнов и смарт-контрактов могут обеспечить надежные одноранговые соглашения и платежные услуги без участия сторонних систем [219];

б) децентрализованность. Блокчейн является оптимальным решением для обеспечения проблем безопасности, конфиденциальности и надежности в среде IoT;

в) целостность данных;

г) устойчивость экосистемы. Отсутствие единой точки отказа позволяет сохранять работоспособность системы в случае сбоя в работе какой-либо ее части.

Шреста, Байрачариа, Нам выделили такие преимущества Блокчейн, как децентрализацию, анонимность, хронологический порядок данных, распределенную безопасность, прозрачность, а также неизменность и пригодность для доверенных сред [257, 303].

Особенность характеристик Блокчейн, а именно неизменный характер сохраняемых цифровых данных, защита от несанкционированного доступа любых контрактов, решений, транзакций и информации привели к пониманию Министерством обороны США перспективы данных технологий в области кибербезопасности [292].

Вместе с тем исследователи выделяют и ряд актуальных проблем широкого внедрения технологий Блокчейн в экономике государств, объединяя их по критериям технических, нетехнических и нормативных ограничений [176].

Бом, Кристин, Эдельман, Мур, Коин, МакМикл выявили следующие ограничения в технологии Блокчейн [304, 305].

1. Отсутствие конфиденциальности. Каждый узел в сети поддерживает полную историю данных транзакций сети. Это может быть атрибутом для конкретных приложений и преимуществом в контексте безопасности, но ограничением для случаев использования, где конфиденциальность является необходимостью. Финансовые учреждения хранят и обмениваются конфиденциальной информацией о своих клиентах и действуют в строгих регуляторных рамках. Согласно Общему положению о защите данных ЕС (GDPR), организации должны получать согласие своих клиентов на использование их частной информации. Вместе с тем при использовании общедоступных систем Блокчейн трудно контролировать конфиденциальность.

2. Высокие затраты. Базовая обработка Блокчейн, где вся история транзакций реплицируется на все узлы, требует больших вычислительных ресурсов. Этот атрибут имеет преимущества безопасности, но может быть ограничением для больших сетей.

3. Модель безопасности. Блокчейн использует шифрование с открытым ключом для транзакционной аутентификации и выполнения.

Этот процесс требует использования открытого и закрытого ключа. Если сторона теряет или невольно публикует свой закрытый ключ, система не имеет механизма для обеспечения дополнительной безопасности.

4. Ограничения гибкости. Неизменяемое добавление только характеристик Блокчейн, гарантирующих целостность транзакций, но может выступать в качестве барьера для случаев использования, которые требуют изменений в транзакциях.

5. Задержка. Принцип работы всех узлов в сети Блокчейн, в которой хранятся полные записи транзакций всех информационных блоков, нарушает учетные данные безопасности сети, однако добавление новых блоков и последующих записей транзакций в настоящее время требует больших затрат.

6. Управление. Распределенная природа архитектуры Блокчейн предлагает конкретные преимущества для конкретных случаев использования, но может быть существенным ограничением для общего контроля и управления со стороны организаций, основанных на надзоре.

7. Системная интеграция.

Нетехнические [176] проблемы в основном связаны а) с созданием легитимности инноваций [306]; б) пониманием факторов, определяющих принятие пользователями новой технологии; в) измерением ценности, получаемой от инвестиций в Блокчейн; г) оценкой потенциального воздействия на общество [307].

Нормативные проблемы возникают 1) из-за распределенной природы приложений Блокчейн, которые могут охватывать несколько юрисдикций, при этом обязанности по обслуживанию системы распределяются между всеми участниками сети [308]; 2) отсутствия признания со стороны юридических и регулирующих органов.

Бисвас и Гупта [309] выделяют такие ограничения реализации технологий Блокчейн в различных отраслях экономики, как проблемы масштабируемости, риски на уровне транзакций, рыночные риски и регуляторные риски, использование на «черном рынке», проблемы конфиденциальности данных, высокие затраты на устойчивость и плохое экономическое поведение.

Одной из проблем внедрения Блокчейн также является отсутствие общепризнанной стандартизации [283, 310]. Вместе с тем международные организации по стандартизации начали формировать некоторые инициативы Блокчейн, например W3C и IEEE, создали

рабочие группы сообщества. ISO создала рабочую группу по технологиям Блокчейн и электронной распределенной книги[20] [267].

В целом, анализируя перспективы внедрения технологий Блокчейн, следует принять во внимание его эволюцию, в рамках которой выделяют четыре этапа [311]:

Блокчейн 1.0 ориентирован на транзакции, в основном на развертывание криптовалют в приложениях, связанных с наличными деньгами, таких как денежные переводы, денежные переводы и системы цифровых платежей [312]. Возможно, наиболее известным примером является Биткойн – децентрализованная цифровая валюта, в которой методы шифрования используются для обеспечения одноранговых транзакций в системе, которая работает без центрального банка или единого администратора. Блокчейн 1.0 напрямую связан с уменьшением стоимости транзакции не только в узком финансовом смысле, но и с более широкой идеей устранения необходимости в центральном органе для обеспечения безопасных транзакций. Такой децентрализованный консенсус снижает затраты, например, за счет устранения посредников.

Блокчейн 2.0 дополнительно включает в себя улучшенную конфиденциальность, смарт-контракты, появление токенов и возможностей, не связанных с нативными активами [313]. Примерами могут служить Ethereum, партнерский Блокчейн IBM-Maersk, поддерживающий глобальные поставки [314] и консорциум Блокчейн торгового финансирования we.trade [315]. Блокчейн 2.0 позволяет разрабатывать и использовать смарт-контракты, Блокчейн больше не ограничивается только финансовыми отношениями. Прозрачная и автономная природа смарт-контрактов снижает риски манипуляций и ошибок.

Блокчейн 3.0 расширяет фокус Блокчейн в направлении децентрализованных приложений (DApp). Приложения DApp разработаны таким образом, чтобы быть гибкими, прозрачными, распределенными, отказоустойчивыми и иметь четкую структуру [316]. Возможность создания децентрализованного хранилища и вычислений

[20] IEEE разработал следующие правила в области Блокчейн: IEEE P2140.1 – общие требования к обмену криптовалюты; IEEE P2140.2 – управление безопасностью для активов и клиентов на биржах криптовалют; IEEE P2140.3 – идентификация клиентов и борьба с отмыванием денег на криптобиржах; IEEE P2140.4 – стандарт для структур обмена активов с использованием DLT (Мир блокчейна и криптовалют: неочевидные тренды-2022. Часть I. – Режим доступа: https://ispace.news/analytics-pro/mir-blokceina-i-kriptovalyut/. – Дата доступа 28.01.2022).

обеспечивает большую масштабируемость приложений. Блокчейн 3.0 меняет более традиционный тип структуры транзакций, поддерживает сетевой подход. Это может повысить инновационность услуг или скорость выхода на рынок новых продуктов. Добавленные функции последующих версий Блокчен позволяют создавать новые рынки и увеличивают потенциальную ценность использования данной технологии.

Блокчейн 4.0 предлагает значительные возможности для создания ценности путем включения AI в технологии Блокчейн[21]. Это позволяет системам принимать решения и действовать по ним без необходимости прямого вмешательства человека. Примерами Блокчейн 4.0 являются DLT сети, построенные на механизмах Solana, Insolar, Aergo, MetaMUI, обеспечивающие крайне низкую стоимость транзакций (0,00025 долларов США для Solana) и масштабируемость в пределах 50 000–1 000 000 транзакций в секунду.

Важно отметить, что драйверами стоимости эволюции технологий Блокчейн последовательно являлись: стоимость транзакций, дополнительные сервисы, организационные границы, автономное принятие решений.

Одной из доминант, определяющих высокую динамику развития цифровой экономики, является концепция AI. Следует отметить отсутствие единого подхода к определению AI в литературе. Группа экспертов высокого уровня по искусственному интеллекту Европейской комиссии предлагает следующее определение для данных систем [318, 319]: «AI относится к разработанным людьми системам, которые функционируют в физическом или цифровом мире, анализируют окружающую среду, интерпретируя собранные структурированные или неструктурированные данные, опираясь на знания, полученные из этих данных, и решая, какие действия следует предпринять (в соответствии с заранее определенными параметрами) для достижения поставленной цели». Важной современной технологией AI является ML[22] [320].

---

[21] Успешным примером такого комбинированного использования технологии является CognitiveScale, стартап AI, поддерживаемый IBM, Intel, Microsoft и USAA, который использует технологию Блокчейн для безопасного хранения результатов приложений AI, созданных для соответствия нормативным требованиям на финансовых рынках [317].

[22] Deep Learning (глубокое обучение) и нейронные сети рассматриваются как передовые методы ML и часто классифицируются отдельно [176].

AI формирует возможности для новых бизнес-моделей и рабочих процессов. Ряд исследователей определили наиболее перспективные направления внедрения технологий искусственного интеллекта, среди которых производство и робототехника, логистика, госуправление, цифровая визуализация, образование, здравоохранение [321]. В исследованиях анализировалось влияние AI и его потенциала для замены людей с помощью интеллектуальной автоматизации в сфере производства, логистике, строительной отрасли. Технологии, ориентированные на AI, смогут отслеживать и контролировать процессы в режиме реального времени, предлагая значительную эффективность по сравнению с ручными процессами [322, 323].

Тесмар, Краер, Пинхеиро, Дэдсон, Величе, Гринберг [324] выделили преимущества использования технологии AI для автоматизации страховых выплат в системе здравоохранения по таким направлениям, как подача претензии, анализ претензий и выявление случаев мошенничества. Исследования, проведенные Juniper, показали перспективы внедрения технологий AI в сферу здравоохранения, производственный сектор и цифровой маркетинг [325].

Ванг прогнозирует, что производственные предприятия будущего будут широко применять технологию искусственного интеллекта, поскольку производство становится более автоматизированным, а промышленность превращается в интеллектуальную платформу, использующую искусственный интеллект и киберфизические системы [326].

Новые варианты бизнес-моделей на основе технологий AI на предприятиях во всех отраслях предлагают прорывные возможности благодаря синергии когнитивных способностей людей и машин [318, 327]:

1) автомобильная промышленность: автономные автопарки, интеллектуальные машины (помощь водителю), прогнозное и автономное обслуживание;

2) энергетика: интеллектуальный учет, более эффективная эксплуатация и хранение энергосистем, интеллектуальное обслуживание инфраструктуры;

3) финансовые услуги: индивидуальное финансовое планирование, выявление мошенничества и отмывание денег, автоматизация транзакций;

4) здравоохранение: диагностическая поддержка на основе данных, обнаружение пандемии, диагностика изображений (рентгенология, патология);

5) производство: усиленный мониторинг и автоматическая коррекция, оптимизация логистики и производства, производство по требованию;

6) розничная торговля: индивидуальный дизайн и производство, создание клиентского опыта, управление запасами и поставками;

7) технологии, коммуникации и развлечения: архивация и поиск медиа, создание контента, персонализированный маркетинг и реклама;

8) транспорт и логистика: автономный транспорт и доставка: регулирование движения и предотвращение заторов, повышение безопасности.

Проведенный анализ показал высокий потенциал использования AI на различных этапах бизнес-процессов на примере таких секторов экономики, как розничные продажи, электроэнергетика и промышленное производство.

Чандринос, Саккас, Лагарос [328] исследовали AI в приложении тестов с использованием данных о торговле на валютном рынке, где комбинация нейронных сетей и методов дерева решений применялась для предоставления трейдерам предупреждений в реальном времени об изменениях в основных торговых моделях во время торговли [176].

AI используется организациями на различных этапах процесса управления рисками, начиная от выявления подверженности риску, измерения, оценки самого риска и его последствий [329]. Более того, данная технология также может оказать содействие в выборе подходящей стратегии снижения риска и найти инструменты, которые могут облегчить последствия наступления прогнозируемых событий. Использование методов искусственного интеллекта для управления операционным риском в настоящее время распространяется на новые области, включающие обнаружение случаев отмывания денег, которое требует анализа больших наборов данных.

По оценкам ряда исследователей, технологии AI будут способствовать увеличению мирового ВВП в среднем на 1,2% к 2030 году.

Ожидается, что мировые расходы на искусственный интеллект вырастут вдвое за четыре года и достигнут 110 млрд долларов в 2024 году. [330]. Согласно докладу института McKinsey, вклад AI в мировую экономику к 2030 году составит 13 трлн долларов США. В том же отчете говорится, что к 2030 году около 70% компаний будут использовать AI [331]. Согласно прогнозу World Economic

Forum (WEF), 20% существующих рабочих мест в Великобритании могут быть затронуты технологиями AI. Этот показатель выше в странах с развивающейся экономикой, таких как Китай и Индия, где этот уровень возрастает до 26% в связи с большими возможностями технологических изменений в производственном секторе [332]. США выделили Министерству обороны в 2017 году 2 млрд долларов для реализации проекта AI Next. Китай в 2017 году инвестировал в данные технологии 12 млрд долларов. К 2030 году Китай, по оценкам Forbes, станет мировым лидером в области искусственного интеллекта [333]. По оценкам WEF, AI к 2030 году обеспечит 20% ВВП Китая [332]. Согласно прогнозам IDC, рынок ИТ-решений на основе AI в Российской Федерации может увеличиться в 80 раз и достигнуть 160,1 млрд российских рублей к 2024 году [334]. Согласно исследованиям Juniper (2019), к 2023 году глобальные расходы на технологии AI только в секторе потребительской розничной торговли достигнут 12 млрд долларов [325]. Две отрасли, которые в прогнозе будут больше всего тратить на AI-решения, – это розничная торговля и банковское дело. Отрасль розничной торговли в основном сосредоточит свои инвестиции в AI на улучшении качества обслуживания клиентов с помощью чат-ботов и механизмов рекомендаций, в то время как банковское дело будет включать расходы на анализ и расследование мошенничества, а также на консультантов по программам и системы рекомендаций [330].

Технологии AI будут стимулировать инновации и экономический рост – 133 млн новых рабочих мест во всем мире [332]. Оценки перемещения рабочих мест из-за автоматизации свидетельствуют, что до трети текущей рабочей деятельности может быть затронуто к 2030 году [335]. Исследования показали, что предприятия будут стремиться направлять работников дальше по цепочке создания стоимости на более творческие и когнитивно-ориентированные роли при поддержке технологий AI [336, 337].

Вместе с тем массовое внедрение технологий искусственного интеллекта может оказать существенное экономическое влияние на организации и учреждения в контексте необходимых инвестиций и изменений в рабочих местах. AI будет оказывать значительное влияние на профессии и виды деятельности в основном по трем каналам [318, 338]:

1) замена человеческого труда: полное поглощение и выполнение работ машинами;

2) повышение эффективности за счет интеллектуального ввода: замена процессов, которые поддерживают фактическое создание стоимости на основе интеллектуальных алгоритмов;

3) новые задачи для предприятий и сотрудников: создание добавленной стоимости за счет выполнения стандартизированных задач компьютерными программами и машинами.

Вместе с тем внедрение AI связано с комплексом сложностей и проблем в экономической, управленческой, социальной, технологической, политической и этической сферах.

Искусственный интеллект является движущим механизмом обработки Big Data (больших данных). Это относительно новая концепция, которую McKinsey определяет как огромные наборы данных, размер которых превышает возможности типичных программных инструментов баз данных для сбора, хранения, управления и анализа [93, 339]. Обработка Big Data (Big data analytics, BDA) относится к инструментам и методам, которые трансформируют большие массивы цифровых данных в аналитическую информацию для принятия управленческих решений [340].

Согласно исследованию Мнини, Ван Бель, Big Data характеризуются несколькими «V»: большой объем (volume), разнообразие типов цифровых данных (variety) и скорость непрерывно генерируемых цифровых данных (velocity) [341].

Демченко, Гроссо, Де Лаат и Мембри к трем характеристикам Big Data добавляют достоверность (Veracity) и ценность (Value) [342]. Саджи и Джейн дополнительно к пяти характеристикам вводят понятие валентности (Valence) и изменчивости (Variability) [343].

В специализированной литературе Big Data также классифицируются по степени, в которой они структурированы:

1) высокоорганизованные и доступные для поиска;

2) неструктурированные (изображения, аудио или видео) [344].

Объем, сложность и разнообразие цифровых данных постоянно увеличиваются. Big Data аккумулируются организациями из различных источников – как внутренних, так и внешних (например, от сотрудников, клиентов, поставщиков и рынков). Каждое цифровое действие ведет к увеличению объема данных, генерируемых с помощью социальных сетей, онлайн-покупок, транзакций, сетевых устройств и образовательных записей [345, 346]. Данный факт формирует проблему нарастающей сложности организации, интерпретации, хранения и анализа большого объема цифровых данных [347].

Цифровая обработка Big Data в сочетании с AI обладает серьезным потенциалом эффективного приложения в таких областях, как промышленное производство, умное здравоохранение, бизнес-аналитика, формируя новые возможности, в том числе в контексте точного прогнозирования [321].

Внедрение технологий аналитики Big Data, по мнению Рагузо, способствует улучшению процесса принятия решений [93, 348].

Безанс приводит несколько направлений аналитики Big Data на уровне организаций, отраслей и госуправления: маркетинг (для сегментации клиентов и анализа на основе рынка), логистика (для анализа цепочки поставок), управление рисками (для моделирования рыночных рисков и выявления мошенничества), расследование мошенничества в сфере социального обеспечения, отмывания денег и т. д. [349, 350].

Многие сектора, среди которых банковское дело, информационные технологии (IT), телекоммуникации, государственное управление, здравоохранение, транспорт, страхование, сектор развлечений, образование, внедряют технологии аналитики больших данных.

Ряд исследователей обосновывают эффективность синергии технологий ML и Big Data в промышленном производстве [351, 352, 353, 354]. Билал, Ойдел, Кадир, Мунир, Айайи, Акинад прогнозируют широкое принятие технологий Big Data в строительной отрасли [355]. Между тем большие данные рассматриваются как «новый тип стратегического ресурса в цифровую эпоху и ключевой фактор, стимулирующий инновации в отрасли, которые меняют текущей способ производства продукции» [356, 357, 358]. Инструменты управления большими объемами информации позволяют организациям создавать более индивидуализированные товары и услуги, способствующие повышению лояльности клиентов и эффективности бизнес-процессов [359].

Использование анализа Big Data предоставляют организациям такие преимущества, как экономия затрат, более эффективное принятие управленческих решений и более высокое качество производимых товаров и услуг [360, 361]. По данным Accenture, организации, которые используют аналитику данных в своих операциях, быстрее и эффективнее реагируют на проблемы логистики и закупок, чем те, которые применяют разовую ad hoc аналитику данных (47% против 18%) [362]. Аналитика Big Data приводит к улучшению точности прогноза показателей спроса, более эффективной

визуализации и отслеживанию поставок в режиме реального времени, а также к более эффективному управлению сетью продаж [363]. Так, аналитика Big Data привела к значительному снижению затрат в розничной торговле.[23] Крупные розничные продавцы используют большие данные для анализа предпочтений и настроений покупателей и повышения количества их покупок.

Инновационные финансовые компании используют данные социальных сетей для оценки кредитного риска и финансовых потребностей потенциальных клиентов и предоставления им новых видов финансовых продуктов. Банки анализируют Big Data, чтобы увеличить доход, повысить удержание и улучшить обслуживание клиентов [364]. Более того, приложения на основе цифровых данных позволяют выявлять риски (атаки) и предотвращать случаи мошенничества [365].

Ли выделил три этапа становления данной технологии после коммерциализации сети Интернет в начале 1990-х годов [360]:

Big Data 1.0 (1994–2004 годы) как интеграция технологий Big-Data и электронной коммерции;

Big Data 2.0 (2005–2014 годы) как интеграция технологий Big-Data и социальных сетей, которые создают новую парадигму функционирования и взаимодействия между организациями и потребителями при относительно низких затратах [366]. Благодаря лучшему пониманию покупателей с помощью аналитики в социальных сетях организации разрабатывают эффективные маркетинговые кампании для целевых сегментов клиентов и адаптируют продукты и услуги к их потребностям и интересам. В отличие от веб-аналитики, используемой в основном для структурированных данных, аналитика социальных сетей используется для анализа данных, которые могут быть естественными, неструктурированными и контекстно-зависимыми;

Big Data 3.0 (2015 – н. в.). Основными участниками Big Data 3.0 являются датчики IoT, которые имеют уникальные идентификаторы с возможностью обмена данными и совместной работы через Интернет без вмешательства человека. Потоковая аналитика извлекает информацию из потоковых данных и используется не только для мониторинга существующих условий, но и для прогнозирования

[23] Например, Tesco, европейская сеть супермаркетов, в результате анализа данных о холодильном оборудовании смогла снизить затраты на электроэнергию примерно на 25 млн долларов в год [367].

будущих событий. Она имеет значительный потенциал в финансовой отрасли, где электронные транзакции должны контролироваться на их соответствие с финансовым законодательством, и в случае выявления подозрительной и мошеннической деятельности инициировать немедленные действия.

Следует отметить, что Big Data выступают не только как инструмент агрегирования и обработки данных, но и как объект торговли. Так, в 2021 году на Шанхайской бирже данных (КНР) стартовали торги Big Data, на которых представлены 20 информационных продуктов в сфере финансов, транспорта и связи[24].

Вместе с тем важно отметить существующие проблемы внедрения данной технологии, связанные с безопасностью и конфиденциальностью цифровых данных [93, 368].

Среди современных технологий, определяющих основные тенденции развития сегодняшней цифровой экономики, следует выделить платформизацию. Большинство крупных технологических компаний в настоящее время можно рассматривать как основанные на платформе предприятия (например, Apple предоставляет аппаратные и программные платформы для других, чтобы создавать приложения. Google предоставляет платформы для объединения рекламодателей и потенциальных покупателей).

В данном контексте важно подчеркнуть разнородность подходов к определению цифровой платформы. Одной из первых внимание новой экономике цифровых платформ уделила Чейз, подчеркнув уникальные свойства данной технологии, которая «...обеспечивает промышленные преимущества значительного масштаба и ресурсов, а “коллеги” объединяют индивидуальные сильные стороны локализации, специализации и настройки, открывая возможности совместной экономики. Когда платформа использует избыточную емкость и в ней участвуют различные партнеры, возникает совершенно новая динамика» [369].

С экономической точки зрения цифровая платформа представляют собой электронную площадку, вокруг которой компании

[24] Контроль над осуществлением биржевых операций поручен одновременно созданному специальному Шанхайскому комитету экспертов по транзакциям с данными. Шанхайская биржа данных — вторая торговая площадка, наряду с Пекинской биржей, которая за последние месяцы открылась в Китае. (В Шанхае заработала новая биржа данных. – Режим доступа: https://bluescreen.kz/news/10095/v-shankhaie-zarabotala-novaia-birzha-dannykh. – Дата доступа:26.11.2021).

и пользователи имеют возможность совместно или по отдельности более эффективно применять инновации и привлекать пользователей. Комплексное определение предложено И. В. Новиковой: «Цифровая платформа – это система алгоритмизированных взаимовыгодных отношений значительного количества независимых экономических субъектов по обмену информацией, созданию и обмену благами, которая приводит к снижению общих транзакционных издержек; оптимизации бизнес-процессов; повышению эффективности цепочки поставок товаров и услуг, осуществляемых в единой информационной среде» [36]. Приведенные определения платформ имеют общее систематическое повторное использование компонентов в разных продуктах семейства продуктов, что позволяет добиться экономии при расширении производства. Следовательно, систематическое создание и использование эффекта масштаба в инновациях можно рассматривать как один из фундаментальных принципов разработки новых продуктов на основе платформы.

Ряд экономистов рассматривают платформы как особые типы рынков («двусторонние рынки», «многосторонние рынки» или «многосторонние платформы»), которые играют роль посредников в обмене между различными типами потребителей, которые иначе не могли бы взаимодействовать друг с другом [370, 371, 372, 373].

Совокупность пользователей платформы составляют ее экосистему, жизнеспособность которой зависит от постоянных инноваций и обслуживания платформы ее владельцем (владельцами) и баланса сотрудничества и конкуренции между поставщиками приложений[25].

Существенной характеристикой многосторонних платформ является наличие «сетевых эффектов», возникающих между «двумя сторонами» рынка. Так, Армстронг определяет двусторонние рынки как «рынки, в которых участвуют две группы агентов, взаимодействующих через «платформы», в которых выгоды одной группы от присоединения к платформе зависят от размера других групп,

[25] В 2020 году Международная организация труда насчитала 777 таких площадок. В странах Европы и Северной Америки, по разным данным, в платформенную занятость включено от 0,3% до 22% взрослого населения. Среди мировых лидеров по этому показателю – Китай, где доля занятых на платформах предположительно достигает 15% от всей рабочей силы. В России около 2 млн человек работают в легальном секторе платформенной занятости и еще порядка 5 млн делают это неофициально. Эксперты ожидают, что платформенная занятость будет расти в сфере электронной торговли, курьерской доставки, персональных услуг и IT. Прогнозы варьируются от 6–8 млн до 15 млн человек к 2030 году [375].

которые присоединяются к платформе» [374]. Платформы создают ценность путем координации групп потребителей, и с экономической точки зрения эта координация осуществляется посредством ценообразования.

В литературе различают два основных типа сетевых эффектов: прямые сетевые и косвенные. Прямые сетевые эффекты, также называемые односторонними сетевыми эффектами, возникают, когда польза от технологии для клиента положительно зависит от числа других потребителей этой технологии.

Косвенные сетевые эффекты и связанное с ними понятие межгрупповых сетевых эффектов отражают существующую базовую взаимозависимость (и взаимодополняемость) между запросами двух или более типов потребителей [376]. Сетевые эффекты иногда характеризуются как эффект масштаба на стороне спроса [377]. Ценность, которую потребители и владельцы платформы могут получить, возрастает с ростом клиентской базы в рамках виртуального цикла косвенных сетевых эффектов. Эти сетевые эффекты, рассматриваемые как существенная особенность платформ, отражают экзогенную взаимозависимость спроса между группами потребителей и формируют конкуренцию платформ. Экономическая точка зрения помогает объяснить, почему некоторые платформы становятся доминирующими и могут даже привести к конкурентным результатам «победитель получает все» в определенных обстоятельствах.

Айзенманн, Заркер, Ван Олстин предложили концепции со стороны предложения, называя платформы «многосторонними сетями», которые имеют как «пользователей на стороне спроса», так и «пользователей на стороне предложения» [378].

В экономической литературе выделяют два основных типа цифровой платформы (а также их гибридные комбинации): первый тип – это инновационная платформа, которая обеспечивает базовую технологию и систему распределения, к которой другие компании могут добавлять свои собственные инновации, повышая ценность системы в целом; второй тип – создает рынок, на котором различные категории пользователей взаимодействуют друг с другом и (или) с самим поставщиком платформы [379].

Платформа цифрового продукта обычно включает в себя определенный диапазон уровней (например, уровни контента и услуг), которые могут функционировать как новый продукт, но одновременно позволяют другим внедрять инновации [138], используя ресурсы

платформы, контролируемые фирмой [111]. Экономика цифровой платформы может быть концептуализирована как совокупность бизнес-моделей с поддержкой технологий, в которых предоставляется платформа, и координирует дальнейшую деятельность пользователей платформы [380].

В экономической литературе цифровые платформы классифицируются по направлению использования на коммерческие и некоммерческие. Некоммерческие, в свою очередь, делятся на обменные, спонсорские, бесплатные услуги и пр. Коммерческие цифровые платформы превалируют в своем разнообразии и подразделяются на платформы электронных платежей, краудфандинговые, социальные, е-коммерции[26].

Платформы дополняют несколько аспектов экономической эффективности взаимодополняющим образом с акцентом на «эффективность распределения ресурсов» – установление цен по рыночному клирингу в отношении спроса и предложения – «информационная эффективность», т. е. степень, в которой цены отражают обоснованные оценки и ожидания прошлого, настоящего и будущего «функциональная эффективность» рынка, т. е. накладные расходы в процессе ценообразования по сравнению с социально-экономической ценностью, которую он обеспечивает [381].

Ввиду распространения цифровых технологий платформы становятся повсеместными, использующими общие стандарты для интеграции продуктов (услуг) и компаний посредством Интернета или частных сетей. Интегрированные цифровые платформы относятся к множеству бизнес-функций и позволяют создавать бизнес-экосистемы [370, 382].

Анализ показывает, что цифровые платформы генерируют как положительные, так и отрицательные эффекты для экономики. Так, одной из важных экономических функций платформ является

[26] По данным немецкой компании Statista, в 2019 году мировой объем e-commerce составлял 3,53 трлн долларов, в 2020 году достиг 4,2 трлн долларов, прогноз на 2021 и 2022 годы составлял 4,9 трлн долларов и 5,7 трлн долларов соответственно (Константинович К. Топ-14 трендов e-commerce на 2021 год. – Режим доступа: https://belretail.by/article/top-trendov-e-commerce-na-god. – Дата доступа: 29.05.2021). По прогнозу eMarketer, в ближайшие годы 52,1% розничных продаж в Китае будет приходиться на электронную торговлю. Впервые в мире большая часть розничных продаж страны будет осуществляться через Интернет. Следующей по доле электронной торговли является Южная Корея, где 28,9% продаж происходит через Интернет. В США показатель составляет всего 15%, а в среднем по странам Западной Европы – 12,8%. Показатель Китая в 2018 году – 29,2% [386].

снижение транзакционных издержек между участниками на разных сторонах рынка. Платформы предлагают сниженные затраты, и повышенное удобство для клиентов, и (или) более низкие барьеры входа для производителей [383]:

Во-первых, это «сетевые эффекты», при которых новые пользователи еще больше повышают привлекательность платформы для других клиентов.

Во-вторых, это масштабирование, основанное на данных, где «больше информации позволяет фирмам разрабатывать более качественные услуги, что привлекает больше пользователей, которые, в свою очередь, генерируют больше данных» [384].

В-третьих, это обычная экономия масштаба, обусловленная преимущественно фиксированной структурой затрат платформ (сама по себе часто является продуктом того, как поставщики могут выбирать, какие затраты следует внедрять, а не извлекать для пользователей).

Платформы могут быстро расти и обслуживать растущее число пользователей, включая клиентов, поставщиков основных и дополнительных услуг, потому что затраты на обслуживание дополнительных пользователей невелики, а в случае цифровых платформ иногда ничтожны [110, 385].

Вместе с тем следует выделить ряд негативных последствий экономики платформ. Обладая информацией, контролируя спрос и фактически владея монополией на цифровую инфраструктуру рынка, собственники платформы начинают контролировать рынок, влияя на ценообразование, способы поставки товаров и услуг, технологии производства, захват цепочки создания добавленной стоимости, формирование новых стандартов от профессий до качества благ, трансформацию самой природы капитализма посредством формирования совместной экономики на цифровых платформах [36].

Цифровые платформы создают условия для стремительного роста компаний, которые их внедряют наиболее активно. Так, большинство компаний с самой высокой рыночной капитализацией в мире – это технологические, получающие большую часть своих доходов от цифровых экосистем, которые они создали [387]. Например, по данным McKinsey, шесть из семи крупнейших компаний – это платформы-экосистемы: Apple, Microsoft, Amazon, Alphabet, Facebook, Alibaba.

По оценкам экспертов McKinsey, такие сектора, как услуги B2B, мобильные услуги, туризм и гостиничный бизнес, здравоохранение и риэлторские услуги к 2025 году могут составить интегрированную сетевую экономику в размере 60 трлн долларов [387].

Следует отдельно отметить влияние платформизации на усиление парадокса, отмеченного Лессигом, обосновавшего специфику характеристик сети Интернет его устойчивостью к вмешательству органов государственного регулирования [388].

Заключение

Таким образом, следует отметить, что анализ проведенных исследований показал эволюционный характер развития и внедрения цифровых технологий, которые легли в основу и трансформируют экономику в направлении цифровизации. В настоящее время, как показал анализ, происходит стадия становления цифровой экономики, связанная с формированием соответствующей экосреды. Представляется, что стадия зрелости цифровой экономики будет связана с конвергенцией комплексных технологических и экономических решений на уровне реализации концепций: Smart City, Intellectual Transport Systems, Industry 4.0, Agriculture 4.0, Smart Supply Chain, Smart Grid, E-Commerce, Telemedicine, FinTech, CBDC, RTGS, E-Government и пр.

Такие технологии, как телекоммуникации, облачные вычисления, IoT, Big Data, AI, расширили информационное общество за счет доступа к различным источникам и большим объемам цифровых данных, создавая условия для коммерческого взаимодействия людей вне зависимости от их географического положения и массива новых автономных цифровых устройств, подключаемых ежегодно. Цифровые технологии, находящие свое отражение во всех элементах экономической системы, оказывают на них трансформирующее воздействие.

1.4. Направления цифровой трансформации экономики и формирование «новой экономики»

Для выделения характеристик и особенностей цифровизации современной экономики представляется целесообразным рассмотреть актуальные тенденции ее трансформации, адаптации к новым цифровым технологиям и концепциям в динамике, с учетом странового и международного опыта имплементации передовых цифровых инноваций в различные элементы экономической системы.

Принято классифицировать рыночную экономику как экономическую систему, основанную на принципах свободного предпринимательства, многообразия форм собственности на средства производства, рыночного ценообразования, договорных отношений между хозяйствующими субъектами, ограниченного вмешательства государства в хозяйственную деятельность [389]. Вместе с тем развитие информационных технологий, их инкапсуляция в традиционные сферы экономики ведут к серьезным изменениям в модели потребления, способах производства, структуре конкуренции и экономической политике, что, в свою очередь, требует разработки новых подходов для анализа их влияния на экономические системы. В 1980-х – 1990-х годах предложена концепция «Новой экономики» в контексте разрушительного влияния IT на экономическое развитие (рис. 1.5) [390].

Концепция «Новой экономики» сформировала подход к экономике как к новому социальному и экономическому порядку, где основным ресурсом является информация. Данные передаются сетями через Интернет, быстро обрабатываются и самостоятельно формируют пространство с помощью компьютерных технологий и программного обеспечения, а затем преобразуются в информацию таким же образом с помощью сетей [100]. Как показано на рис. 1.5, концепция «Новая экономика» имеет четыре определяющих элемента: цифровизацию, глобализацию, НИОКР и квалифицированные человеческие ресурсы. Эти элементы влияют друг на друга и создают новую экономическую структуру [391]. Глобализация с точки зрения концепции «Новой экономики» ведет к устранению национальных границ и размыванию парадигмы национального государства. Роль географического расстояния меняется, поскольку стоимость транспортировки цифровых товаров и информации приблизительно равна нулю [392]. В рамках данной концепции источником богатства являются не природные ресурсы и физический труд, а информация и связь. Постоянные инновации в Интернете, программном обеспечении, коммуникациях и информационных технологиях необходимы для непрерывного роста в Новой экономике. Цифровизация, конвергенция цифровых технологий для улучшения бизнес-процессов и повышения эффективности как на уровне конкретных предприятий (отраслей), так и экономики в целом приводят к бифуркации, качественно отличному поведению элементов экономической системы и количественному изменению ее параметров.

Рис. 1.5. Развитие концепции
«Новой экономики 2.0» (разработано автором)

Новая экономика 2.0 охватывает не только традиционные сектора, которые активно осуществляют цифровизацию бизнес- и технологических процессов, формируя новую экономическую среду, новые экономические механизмы и институты. Формируются и совершенствуются цифровые экономико-технологические концепции, характеризующие трансформацию Новой экономики в Новую экономику 2.0: Smart City, Industry 4.0, Agriculture 4.0, Smart Supply Chain, Smart Grid, Intellectual Transport Systems, E-Commerce, Telemedicine, включающие различные подкомпоненты и концепты: Smart Construction, Smart Buildings, VANET, Precision Agriculture, Smart Farming, Smart Factory, Colobots, Additive Manufacturing, Digital Twins, Cloud manufacturing, Distributed Manufacturing и пр. (рис. 1.6) по мере приближения цифровой экономики к стадии зрелости.

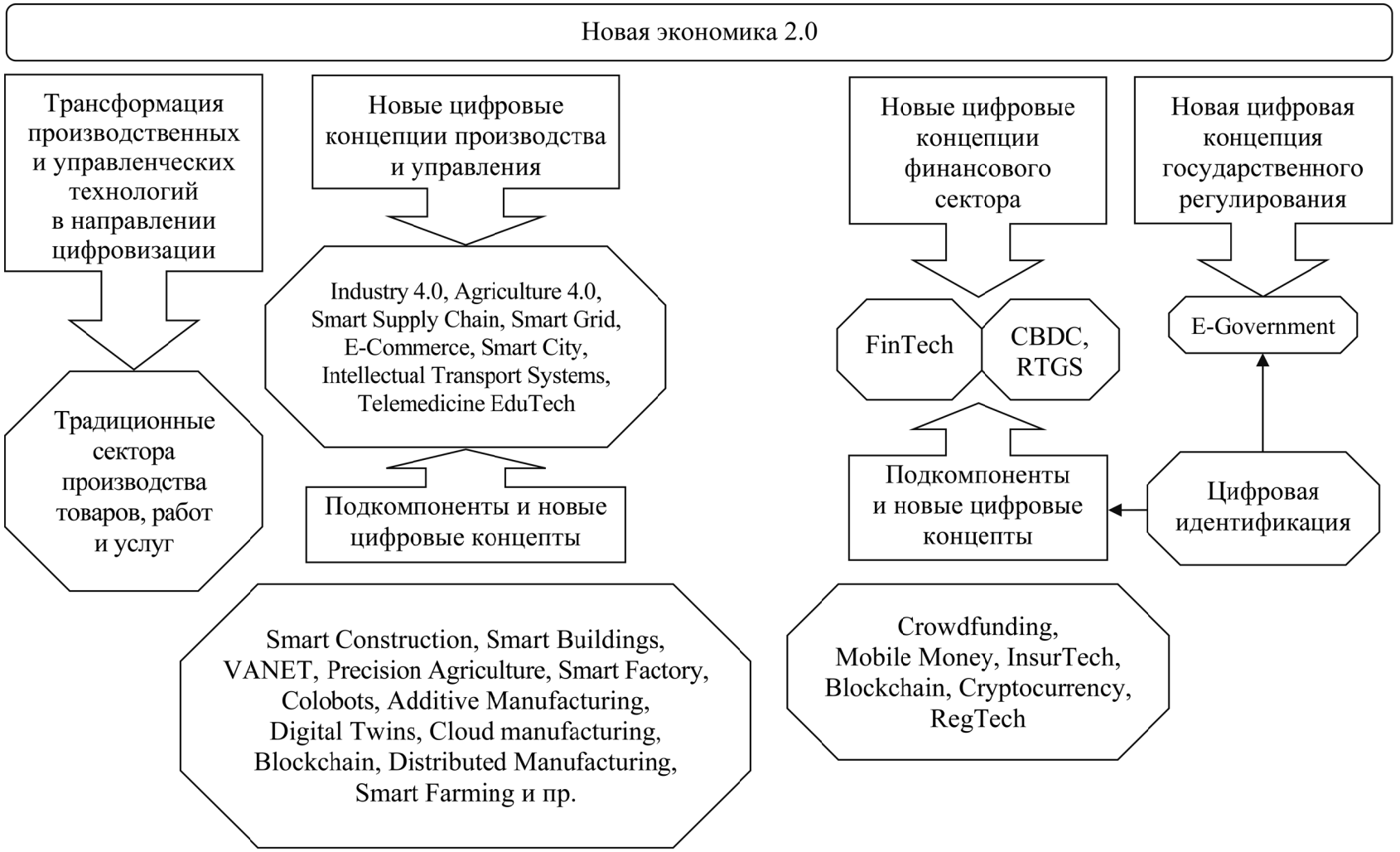


Рис. 1.6. Составляющие Новой экономики 2.0 (разработано автором)

В рамках данного исследования следует отметить, что любая экономическая система может рассматриваться как образование, состоящее из двух систем – производственной и финансовой, в которых система производства является первичной, или базовой, а финансовая система, возникшая для удобства функционирования производственной системы – вторичной. Финансовая система призвана обеспечить гибкость и оперативность производственной системы и является ее надстройкой [393]. Элементами, характеризующими современное направление развития цифровой экономики в области финансовых услуг, являются FinTech, CBDC, RTGS. Цифровизация государственного регулирования характеризуется концепцией E-Government.

В секторе производства цифровая трансформация экономики и общества находит отражение в фундаментальных изменениях производственных процессов, экономических моделей, взаимодействии с поставщиками и клиентами при реализации концепции Industry 4.0 (I4.0), характеризуемой рядом ученых как революционный процесс [394]. Данная концепция имеет эволюционный характер, поскольку основана на предыдущих этапах и развивает автоматизацию в направлении реализации киберфизических систем и взаимодействия человека с машиной. В дополнение к повышению автоматизации она охватывает интеллектуальные процессы для управления и контроля производственными процессами в отдельных компаниях, а также по всей цепочке создания стоимости и в сетях. Это подразумевает смещение управления производственным процессом с центрально-ориентированной точки на сетевую перспективу с различными отдельными этапами производства, управляемыми интеллектуальными элементами и продуктами [395, 396, 397, 398, 399]. Конвергенция производственных, вычислительных и коммуникационных технологий создала новые возможности для более быстрого, дешевого и умного производства [399, 400].

Концепция I4.0 разработана в 2011 году в интересах немецкой промышленности для характеристики новой стратегии, описываемой гибкими производственными системами на основе платформизации и Интернета. Данная концепция охватывает не только производственные источники, т. е. машины, датчики и роботов, которые связаны друг с другом, обмениваются информацией, прогнозируют и обслуживают сами себя, но и продукты или услуги, клиентов и бизнес-модели [401]. Важнейшим компонентом I4.0 являются киберфизические

системы (CPS), которые позволяют интегрировать физические процессы с вычислениями через встроенные вычислительные устройства и контуры управления с обратной связью [396, 402]. Производственная концепция I4.0 описывает систему, поддерживающую [399]:

1) интегрированные совместные цепочки создания стоимости, которые организуют и совместно используют производственные ресурсы через Интернет;

2) цифровизацию и интеграцию производственных ресурсов в IoT в качестве адаптивных, безопасных и предоставляемых по требованию микросервисов;

3) интеллектуальные и связанные объекты CPS, способные принимать решения в режиме реального времени и автономно благодаря встроенной электронике, и аналитические (когнитивные) услуги.

Функции I4.0, включающие в себя горизонтальную интеграцию (для облегчения сотрудничества между компаниями), вертикальную интеграцию иерархических подсистем (для повышения гибкости производственной линии) и сквозную инженерную интеграцию, поддерживают настройку продукта на протяжении всей цепочки создания стоимости и формируют сервисно-ориентированное производство [403]. По данным исследования ABI Research, промышленные предприятия могут ожидать десятикратного увеличения рентабельности инвестиций (ROI) в мобильные технологии Industry 4.0, в то время как складские сервисы – 14-кратного увеличения ROI [404].

Вместе с тем следует отметить развитие данной концепции, ее адаптацию к меняющимся экономическим условиям и совершенствованию технологий. При этом аналогом I4.0 в экономической литературе является также термин Smart manufacturing. Согласно определению Национального института стандартов и технологий США (NIST), Smart manufacturing – это «полностью интегрированные, совместные производственные системы, которые реагируют в режиме реального времени, чтобы удовлетворить меняющиеся требования и условия на заводе, в сети поставок и в потребностях клиентов» [405]. В США данная производственно-цифровая интеграция также получила название Industrial Internet of Things (IIOT) [406]. В Испании Министерством промышленности, торговли и туризма предложена концепция Connected Industry 4.0, предполагающая многоуровневую систему, включающую элементы внутри и межфирменных цифровых приложений управления, сетевой обработки данных и киберфизической экосистемы.

Ряд исследователей в качестве элемента I4.0 выделяют концепцию Smart Factory, которая опирается на программные системы для планирования и контроля производственных процессов и управления цепочками поставок [407, 408, 409, 410]. Smart Factory – это интеллектуальное производственное решение, которое обеспечивает гибкие и адаптивные производственные процессы для решения проблем на промышленных объектах [199]. Это решение может быть связано с автоматизацией и рассматриваться как сочетание программного, аппаратного и механического.

Таким образом, с учетом комплексности техно-экономических задач, решаемых в рамках концепции I4.0, ключевыми технологиями, определяющими развитие Industry 4.0 на современном этапе, являются:

1) IoT в производстве (предоставление удаленным устройствам возможности общаться и взаимодействовать между собой и с централизованными контроллерами, обеспечивая возможность реагирования в реальном времени);

2) Cloud Manufacturing (организация производственных ресурсов по сетям (производственным облакам) в соответствии с потребностями потребителей для осуществления «производства по требованию»);

3) Additive Manufacturing (интеграция 3D-печати в производственных процессах);

4) моделирование (создание «цифровых близнецов», позволяющее своевременно управлять данными с помощью виртуальных моделей продуктов, материалов и производственных процессов);

5) системная интеграция (формирование киберфизических систем, использование AI);

6) автономная и совместная робототехника (применение в производстве коллаборативных роботов (collaborative robots, или cobots) [411];

7) AI и аналитика Big Data (направленные на использование в качестве поддержки в принятии решений в режиме реального времени);

8) Smart Supply Chain в рамках обеспечения производственных процессов;

9) промышленный Блокчейн (для хранения и обработки цифровых данных);

10) кибербезопасность.

Анализ перспективных технологий, интегрируемых в рамках I4.0, следует начать с концепции Colobots, которая в развитии технологий робототехники предполагает использование автономных и совместно используемых роботов (коллаборативных роботов). Совместная (коллаборативная) робототехника перераспределяет выполнение тяжелых или повторяющихся задач от рабочих в пользу автоматизированных систем. В ситуациях, когда существует нехватка рабочей силы, производительной мощности или низкие эффективность и производительность в повторяющихся процессах, совместная робототехника является оптимальным дополнением к функционалу сотрудников [412]. Среди потенциальных преимуществ автономных роботов следует выделить повышение эффективности и производительности производства, уменьшение количества ошибок, снижение риска травм и повышение безопасности работников, повышение удовлетворенности клиентов качеством поставки товаров[1] [413, 414]. Вместе с тем важно отметить основное ограничение использования данной технологии, которым является обеспечение абсолютной безопасности производства. Вместе с тем новые технологические разработки в данной сфере направлены на снижение травматизма и повышение эффективности работы персонала[2]. Согласно отчету Международной федерации робототехники (IFR), в 2020 году в мировом производстве было задействовано 3 млн промышленных роботов, работающих на заводах по всему миру. Ожидается, что в ближайшее время количество поставок роботизированных систем во всем мире вырастет на 13% до 435 тыс. единиц. Азия остается крупнейшим в мире рынком промышленных роботов. 71% всех вновь развернутых роботов в 2020 году были установлены в Азии, высокие темпы роста указывают на быструю скорость роботизации в Китае [415].

---

[1] Проведенное исследование показало, что интегрированные команды роботов и людей (коботы) на 85% более производительны, чем по отдельности роботы или люди [414].

[2] Amazon тестирует четыре новых складских робота, чтобы сократить травматизм своих работников в распредцентрах на 50% к 2025 году. В 2021 году компания инвестировала в проекты по обеспечению безопасности труда рабочих более 300 млн долларов. В 2019 году Amazon зарегистрировала 14 000 таких серьезных травм среди персонала на 150 своих складах. Это на треть больше, чем было в 2016 году, и почти вдвое превышает стандарт в отрасли (Amazon «примет в штат» четыре новых типа роботов. – Режим доступа: https://logirus.ru/news/warehouses/amazon_primet_v_shtat-_chetyre_novykh_tipa_robotov.html. – Дата доступа: 15.06.2021).

Существенным компонентом I4.0 является также концепция Additive Manufacturing («Аддитивного производства», также называемая 3D-печатью), позволяющая изготавливать сложные кастомизированные конструкции. Additive Manufacturing является одной из наиболее разрушительных технологий, представленных в контексте I4.0 [22]. Этому разрушительному потенциалу способствуют две характеристики технологии: во-первых, она позволяет напрямую создавать физические объекты из цифровых данных дизайна, что также предоставляет новые возможности для свободы проектирования. Во-вторых, на стороне потребителей аддитивное производство позволяет частным и промышленным пользователям разрабатывать и производить свои собственные товары, усиливая концепцию Тоффлера [416] и Котлера [417] о prosumer (индивидууме, который выступает одновременно и как производитель, и как потребитель) [418, 419].

По мнению ряда исследователей [418, 420, 421, 422], данная концепция окажет существенное влияние на технологические и бизнес-процессы в производстве, при разработке цепочек поставок и логистики, планировании жизненного цикла продукта, поведение потребителей. Additive Manufacturing позволяет сократить число поставщиков и оказать положительное влияние на качество и количество трудовых ресурсов [423]. Вместе с тем растущие требования к разработке дизайна продукции предполагают внедрение новых производственных процессов, технологий планирования и контроля качества [420].

Прогнозы исследовательского центра Delphi на 2030 год в отношении развития данной технологии свидетельствуют о следующем:

1) в промышленности значительно увеличится Additive Manufacturing, локализованное вблизи фокусных групп потребителей, что приведет к сокращению глобальных производственных цепочек;

2) реализация конечных продуктов более чем на 25% переместится в сферу продажи цифровых файлов вместо продажи физического продукта;

3) важной нормативной мерой станет регулирование платформ обмена файлами для Additive Manufacturing;

4) производство запасных частей будет разделено на две системы: менее важные детали будут производиться на месте с помощью Additive Manufacturing, тогда как критические детали будут изготавливаться в специализированных центрах с особыми квалифика-

ционными навыками (контролем качества), в основном с использованием традиционных технологий производства;

5) рыночная доля изделий (продуктов, компонентов), произведенных в Additive Manufacturing, превысит 10% во всех отраслях [418].

Составной частью концепции I4.0 является моделирование, позволяющее своевременно управлять данными с помощью виртуальных моделей продуктов, материалов и производственных процессов. В этом контексте важно отметить развитие концепции Digital Twins – «цифровых близнецов», которые являются виртуальными копиями физических устройств для запуска симуляций[3] [424, 425]. Фактически, это промышленная реализация киберфизической системы (CPS). Большинство крупных компаний-производителей (GE, Chevron, Schneider Electric и др.) уже вводят в производственные процессы Digital Twins [4] [426].

Концепция Digital Twins была впервые внедрена в области авиастроения и космической промышленности в качестве модели информационного отзеркаливания для анализа состояния оборудования в режиме реального времени и для получения точных данных для принятия управленческих и технологических решений[5] [351, 427].

Важным компонентом I4.0 является концепция Cloud manufacturing («облачного производства»), предполагающего интеграцию промышленного производства с IoT и вычислительными технологиями [428, 429]. Главной особенностью данной концепции является преобразование производственных ресурсов и мощностей в услуги. Cloud manufacturing, также называемое сервис-ориентированным производством [399, 431], относится к парадигме «сетевого производства», которое организует производственные ресурсы по сетям

[3] Другими словами, цифровой близнец – это компьютерная программа, которая принимает реальные данные о физическом объекте или системе в качестве входных данных и создает выходные данные для прогнозирования или моделирования того, как эти физические объекты или системы будут затронуты этими входными данными.

[4] В аналогичном контексте используется термин «Digital Shadow», который предполагает «достаточно точное» отображение процессов «в производстве, разработке и смежных областях с целью создания базы анализа в реальном времени для всех соответствующих цифровых данных» [426].

[5] В промышленном производстве данная концепция реализуется посредством непрерывного аккумулирования виртуальной цифровой фабрикой данных в реальном времени с физической производственной линии, а также исторических данных для обучения, проверки и обновления моделей и в конечном итоге предоставления обратной связи промышленному предприятию для производственного контроля. Гривс предложил использовать данную концепцию для управления жизненным циклом продукта (PLM) [430].

(производственным облакам) в соответствии с потребностями потребителей для осуществления «производства по требованию», предоставления услуг через сети (Интернет) и сервисные платформы Cloud manufacturing»[6] [428]. Ряд исследователей [429, 432] выводят комплексное определение данной концепции: Cloud manufacturing – это новая, сетевая и интеллектуальная модель производства, ориентированная на обслуживание, знания, высокую производительность и энергоэффективность. В этой модели современные технологии, такие как цифровое производство, облачные вычисления, IoT и высокопроизводительные вычисления, интегрированы для обеспечения безопасных, надежных и высококачественных услуг по требованию при низких ценах для тех, кто участвует во всем жизненном цикле производства. Отмечается необходимость интеграции облачного производства и CPS для предоставления производственных услуг, которые могут напрямую управлять и контролировать станки в производственном облаке. Создается новая парадигма «облачного киберфизического производства» (cyber physical manufacturing cloud, CPMC), в которой инструменты обработки могут напрямую контролироваться и управляться через Интернет из облака [428]. Вместе с тем ограничением принятия данной парадигмы является выявление определенной части локальной физической вычислительной мощности для переноса в облачные системы, поскольку проблемы с безопасностью данных, внутренними политиками ИТ или даже возможностью банкротства облачной компании могут воздействовать на данные, хранящиеся в облаке, ограничивая их использование [433].

Следует также отметить актуальность проблематики интеграции технологий Блокчейн в концепцию I4.0. Промышленный Блокчейн можно определить как использование технологии Блокчейна в отрасли с интеграцией IoT, M2M и эффективных алгоритмов децентрализованного консенсуса для удовлетворения требований безопасности, открытости и децентрализации [434]. Смарт-контракты используются для облегчения выполнения транзакций и сервисов в рамках жизненного цикла продукта, а технологии IoT – для сбора и мониторинга соответствующих цифровых данных[7].

---

[6] Расширением этой парадигмы являются облачные проектирование и производство, представляющие собой «сервис-ориентированную модель разработки сетевых продуктов», в которой потребители услуг могут настраивать, выбирать и использовать специализированные ресурсы и услуги по реализации продуктов [435].

[7] Ряд исследователей предложили децентрализованную одноранговую платформу BPIIoT для промышленного IoT, основанную на технологии Блокчейн [436].

Важнейшим элементом I4.0 является Smart Supply Chain (цифровая цепочка поставок), которая включает в себя все виды деятельности, связанные с потоком и преобразованием продукта, услуг и информации, от сырья до конечного потребителя[8]. В рамках I4.0 основная цель Smart Supply Chain – полная цифровая интеграция, при которой каждое движение продуктов, работ и услуг отображается в системах всех участников поставки в режиме реального времени, беспрепятственный отзыв продукции, повышение эффективности производственного процесса для снижения затрат, управление характеристиками продукта на основе обратной связи с клиентом, повышение качества товаров, работ и услуг, формирование оптимальной цены, улучшение обслуживания клиентов. Цель цифровой интеграции – предотвращение перехода данной системы в нежелательное состояние [437]. Цифровизация логистики поставок направлена на ускорение процесса принятия решений; лучшее реагирование на меняющиеся потребности рынка; снижение рисков; повышение внутренней / внешней прозрачности и, как следствие, рост показателей эффективности производства за счет сокращения эксплуатационных расходов, улучшения качества продукции; повышение прозрачности и эффективности продаж, создание новых возможностей для развития бизнеса и создание стратегических преимуществ [438]. Цифровые технологии позволяют отслеживать движение товаров, определять неэффективность производства и жизнеспособность товаров, отношения с поставщиками, формировать прогнозы и запасы, определять актуальные тенденции на основе данных, предоставленных датчиками [439, 440].

Важно отметить перспективность интеграции в цепочку поставок технологий Блокчейн, что позволит гарантировать качество продукции, повысить надежность и прозрачность поставок, улучшить обмен информацией между деловыми партнерами [283, 438, 441]. Блокчейн-интеграция компаний, включенных в цепочку поставок,

[8] Управление цепочками поставок (SCM, Supply Chain Management) включает планирование и управление всеми видами деятельности, связанными с поставками, закупками, конверсией и всеми действиями по управлению логистикой. Важно отметить, что это также включает в себя координацию и сотрудничество с партнерами по каналам, которые могут быть поставщиками, посредниками, внешними поставщиками услуг и клиентами. По сути, управление цепочками поставок интегрирует управление спросом и предложением внутри компаний и между ними [447]. Цепочка поставок обладает наибольшим потенциалом для экономии затрат и повышения эффективности в любой отрасли [425].

товарных потоков, логистики, потоков капитала и информационных потоков может снизить эксплуатационные расходы и повысить качество работы предприятий[9] [442, 443]. Исследователи отмечают следующие управленческие преимущества Блокчейн в рамках Smart Supply Chain [444, 445, 446]:

1) снижение транзакционных издержек / времени в результате использования платформ Блокчейн, которые не требуют участия третьих сторон;

2) улучшение видимости по всей цепочке поставок;

3) улучшение связи между торговыми партнерами.

Кроме того, использование Блокчейн для Smart Supply Chain обеспечивает [448]:

а) сокращение контрафактной продукции (предоставление сведений о происхождении продукта помогает партнерам отслеживать создание продукта, его ингредиенты, сведения о владельце и хранении, тем самым устраняя контрафактную продукцию);

б) цифровизацию данных о продукте: сведения о продукте и его жизненный цикл хранятся в системе в цифровом формате, что устраняет сомнительность в отношении происхождения и качества продукта;

в) ускорение операций: прозрачный аудит улучшает соблюдение государственных норм и ускоряет таможенное оформление (Блокчейн устранит необходимость в файлах для отчетов о странах происхождения и других таможенных / пограничных документах. Информация станет доступна в Блокчейн для мгновенного доступа правительственных учреждений);

г) более высокие темпы роста предприятий (прозрачность бизнес-операций для заинтересованных сторон и партнеров будет способствовать устойчивому росту благодаря неизменному, безопасному и взаимному обмену данными);

---

[9] Испанский производитель морепродуктов Nueva Pescanova объявил о сотрудничестве с технологическим гигантом IBM для отслеживания цепочки поставок. Место и время вылова, маршрут доставки и другие сведения о морепродуктах будут храниться на платформе IBM Food Trust на базе Блокчейна. Инициатива создаст сеть между рыболовами, производителями и дистрибьюторами, что повысит эффективность поставок, сократит риски мошенничества и предоставит потребителям достоверную информацию о происхождении продукции. Южнокорейская авиакомпания Jeju Air заключила сотрудничество с дочерней фирмой LG по IT-услугам LG CNS для исследования Блокчейн-решений в авиационной промышленности. Компании разрабатывают совместный пилотный проект для технического обслуживания самолетов (Быков А. Управление авторскими правами, техобслуживание самолетов и другие блокчейн-инициативы. – Режим доступа: https://forklog.com/upravlenie-avtorskimi-pravami-tehobsluzhivanie-samoletov-i-drugie-blokchejn-initsiativy/. – Дата доступа: 19.06.2021).

д) повышение качества информации (подключение в рамках Блокчейн большого количества корпоративных систем, таких как ERP, MES и т. д., создаст условия для повышения доступности и качества цифровых данных).

Более того, используя Блокчейн, предприятия с обширной логистической сетью имеют возможность идентифицировать источники потенциальных рисков, таких как загрязненная продукция, дефектные детали и мошеннические схемы поставки [438].

В настоящее время ключевые проблемы интеграции Блокчейн в Smart Supply Chain связаны со значительными финансовыми затратами, сложной сетевой инфраструктурой и правовыми аспектами, что включает следующие элементы.

1. Инфраструктура и сеть. Блокчейн нуждается в онлайн-транзакциях, связи и хранении данных. Это требует значительной пропускной способности Интернета и мощности обработки цифровых систем, что представляется затруднительным в развивающихся и слаборазвитых странах.

2. Функциональная совместимость. Блокчейн должен иметь возможность беспрепятственно работать в ERP и других системах в условиях свободного доступа, надежной связи и скоростной передачи информации между различными корпоративными системами управления.

3. Затраты на адаптацию и обслуживание. В Smart Supply Chain с поддержкой Блокчейн узлы являются партнерами в цепочке поставок, то есть поставщиками, клиентами, дистрибьюторами и производителями. Загрузка и поддержка этих кодов, особенно для транзакций с большими объемами, имеют значительную стоимость.

4. Стоимость хранения данных на Блокчейн. Данные Блокчейн хранятся в облаке. База данных Блокчейн должна хранить данные неопределенно долго, а такое бессрочное хранение данных требует больших затрат.

5. Задержка проверки данных. Задержка в передаче информации должна исчисляться секундами.

6. Ограничение размера полезной нагрузки. Существует ограничение размера полезной нагрузки для любой сети Блокчейн, открытой или закрытой.

7. Нормативно-правовое регулирование. Блокчейн не имеет правовой базы. Органы государственного управления в различных юрисдикциях имеют диаметрально противоположные подходы по проблематике Блокчейн.

8. Доверие. Центральным условием внедрения Блокчейн является необходимость доверия между партнерами.

Важно отметить, что управление цепочкой поставок представляет собой сектор стоимостью 16 трлн долларов США. Составляющими расходов сектора являются высокие затраты на обработку ошибок, предотвращение мошенничества и администрирование [449, 450]. Цифровизация цепочки поставок Cisco позволила компании увеличить производительность на 35% и сэкономить 40% на капитальных затратах. Cisco улучшила свою способность выполнять обязательства по доставке товаров клиентам на 5–10% с точки зрения запланированного времени выполнения заказа. Среди прочего, в решениях для Smart Supply Chain используются технологии AI и IoT, которые помогли таким клиентам, как Microsoft, сократить запасы на 200 млн долларов, Lennox – на 90% меньше времени, необходимого для сбора данных, и повысить эффективность цепочки поставок Komplett Group на 28% [438, 451, 452]. Ежегодная экономия на транспортных расходах транспортно-логистических компаний за счет IT-решений может составить от 2,5 до 30% в зависимости от количества перевозок, направлений и применяемых форм оплаты[10] [453]. В год количество складских роботов увеличивается более чем на 60% и к 2022 году достигнет около 1 млн экземпляров против 200 тыс. в 2018 году. Даже частичное внедрение роботов позволяет повысить производительность. Кроме того, роботизация помогает до 4–5 раз уменьшить рабочий цикл и существенно сократить операционные расходы склада [454].

В 2019 г. компании Maersk и IBM объявили «TradeLens»[11], глобальную торговую платформу, основанную на Блокчейн, с более чем 90 первоначальными участниками, включая операторов портов и терминалов, перевозчиков, владельцев грузов, экспедиторов и другие логистические компании [283, 455, 456]. Порт г. Хьюстона (США), Роттердамская система сообщества портов (Нидерланды), таможенная администрация Нидерландов и таможенная и пограничная служба США будут частью этой сети Блокчейн [448, 457]. В 2017 году корпорация Samsung запустила консорциум Блокчейн,

[10] Внедрение цифровой платформы «Умной логистики» в «Мосстрое-31» (РФ) дало экономию на логистике 2 млн российских рублей в месяц (при среднегодовых тратах на нее 120–130 млн российских рублей).

[11] Платформа облегчает спотовые рынки и, следовательно, более ориентированные на рынок структуры управления, поскольку затраты на координацию сокращаются. Таможенные органы также включены в платформу TradeLens.

в который входит Корейская таможенная служба и Корейское министерство океанов и рыболовства. Другим примером является порт г. Антверпена (Бельгия), который тестирует использование Блокчейн для автоматизации и оптимизации контейнерных логистических операций на своем терминале. Французский автопроизводитель Renault [458] использует Блокчейн-решение на основе Microsoft Azure для управления информацией о владении автомобилем и его обслуживании, отслеживания его продуктов на рынке и упрощения выпуска новых моделей.

Составным элементом концепции I4.0 является «Распределенное производство» («Distributed Manufacturing» (DM), которая формируется как «способность персонализировать производство продукции в разных масштабах и местах, в точке потребления, продажи и в форме децентрализованного производства, практикуемой фирмами, использующими сеть географически распределенных производственных мощностей, которые координируются с использованием цифровых технологий (IoT и Big Data и т. д.) и новых технологий производства» [459, 460]. К преимуществам распределенного производства следует отнести 1) снижение негативного воздействия производства / транспорта на окружающую среду; 2) повторное использование и укрепление локальной промышленности и экономической среды [461, 462, 463].

Вместе с тем следует выделить ряд проблем, препятствующих реализации концепции I4.0, в частности отсутствие стандартизации систем в условиях гетерогенности экосистемы IoT, состоящей из множества различных компонентов[12] и заинтересованных сторон [464, 465, 466]. Барьером внедрения концепции I4.0, как показал анализ, подготовленный в компании Bosch, является отсутствие системы образования, сопротивление сотрудников технологическим и управленческим изменениям[13], трудности в поиске квалифицированных специалистов [467]. В этом исследовании также делается вывод о том, что критическим препятствием для реализации I4.0 является отсутствие ресурсов для инвестирования. К проблемным аспектам следует также отнести информационную безопасность[14].

[12] Меток NFC, датчиков, микрокомпьютеров, мобильных гаджетов, промышленных роботов, домашних устройств, транспортных средств.

[13] Аналог стихийным протестам луддитов в XIX веке против внедрения машин.

[14] В связи с растущей оцифровкой процессов, машин и оборудования отмечается высокий риск кибератак на фабричные информационные системы, информация о дизайне продукта и сотрудниках может быть доступна для промышленного шпионажа.

Технологическим ограничением является отсутствие устойчивой и широкополосной скоростной сети (5G).

С целью продвижения концепции I4.0 сближение традиционного промышленного производства с IT и новыми технологиями, такими как IoT, кроме Германии, на государственном уровне инициированы Европейской комиссией в рамках программы «Factories of the Future» (FoF) [411, 468, 469].

Кроме того, Европейская комиссия в 2012 году определила шесть приоритетных областей, имеющих огромный потенциал для роста и создания рабочих мест в Европе [400, 432]. Две из этих областей имеют непосредственное отношение к I4.0: продвижение «передовых производственных технологий» («advanced manufacturing technologies») и «ключевых технологий поддержки» («key enable technologies»). Великобритания признана лидером по направлению развития интеллектуальных услуг в I4.0 [470], кроме того, Соединенное Королевство осуществляет проекты «Future of Manufacturing» и «Catapult» [471]. Во Франции в рамках внедрения технологий I4.0 реализуются проекты «Industrie du Futur», «La Nouvelle France Industrielle» [472], Нидерландах – «Smart Industry» [473], Италии – «Impresa 4.0» [474], Португалии – i4.0 [475]. В Бразилии правительство поддерживает Industry 4.0 в рамках «Национального плана коммуникации M2M и IoT» [394]. Казахстан активно работает над внедрением Индустрии 4.0 как элемента повышения конкурентоспособности[15]. Республика Корея реализует проекты «Manufacturing 3.0» и «Smart Factory Initiative» [476, 477]. Индия осуществляет проект «Make in India», включающий компоненты как I4.0, так и общей цифровизации экономики [478]. Китай реализует программы «China Manufacturing 2025», «Made in China 2025», «Internet Plus», способствующие глубокой интеграции информатизации и индустриализации и ускорению развития передового производства и экономики [199]. В 2016 году в стране основан Альянс промышленного Интернета (Alliance of Industrial Internet – AII), целью которого является создание общественной платформы для продвижения цифровизации управления, производства, обучения, внедрение новых информационных технологий и промышленных систем[16]. Соединен-

[15] Недавно запущенная Государственная программа «Цифровой Казахстан» нацелена на ключевые области, такие как развитие высокоскоростной, безопасной цифровой инфраструктуры, создание компетенций и навыков для цифровой экономики и цифровое преобразование экономики как таковой.

[16] http://en.aii-alliance.org/

ными Штатами в 2011 году начата правительственная инициатива «Advanced Manufacturing Partnership – AMP», направленная в том числе на объединение CPS, IoT, автоматизацию, Big Data и Cloud computing для достижения синергии данных и устойчивого производства. Цель инициативы – объединить промышленность, университеты и федеральное правительство для инвестирования в новые технологии с целью создания высококачественных производственных рабочих мест и улучшения национальной конкурентоспособности [479].

На международном уровне технический совет Международной организации по стандартизации (International Standard Organization – ISO) в г. Женева учредил в 2015 году стратегическую консультативную группу (Strategic Advisory Group – SAG) по разработке Industry 4.0/Smart Manufacturing. Одной из основных задач SAG является согласование точного определения Industry 4.0 [432, 480].

На уровне предприятий реализацию концепции I4.0 осуществляют в рамках Промышленного Интернет-консорциума (Industrial Internet Consortium – IIC) пять ведущих производственных компаний США, в том числе AT&T, Cisco, GE, IBM и Intel. Целью IIC является устранение технических барьеров и содействие интеграции физического и цифрового миров, направленных на производство инновационных продуктов и систем в области интеллектуального производства, здравоохранения, транспорта и др. [202]. В 2017 году IIC опубликовал отчет «Промышленная эталонная архитектура Интернета», который представляет базирующийся на стандартах шаблон и методологию построения системы промышленного Интернета вещей (IIoT) на основе общей концепции и структуры, включающий шесть руководящих принципов I4.0 [481]:

1) функциональная совместимость (между CPS и людьми);

2) виртуализация (с помощью которой CPS контролируют производство);

3) децентрализация (когда CPS принимают независимые решения);

4) возможности выполнения анализа в реальном времени (для изучения производственных данных);

5) ориентация на обслуживание (внутреннее, а также предложение индивидуализированных услуг и продуктов);

6) модульность (адаптация в реальном времени к динамическим изменениям потребительского спроса, заводских настроек и сетей снабжения и цепочек создания стоимости).

В рамках проекта Глобальная сеть маяков (Global Lighthouse Network –GLN) с 2018 года ведущие производственные компании[17] работают над реализацией потенциала инноваций и достижений инновационной экономики. В настоящее время GLN включает 54 проекта в таких секторах, как биотехнологии, нефтегазовый сектор, аддитивное производство, электронные компоненты, сельскохозяйственное, медицинское оборудование, потребительские товары, станкостроение, фармацевтика, сталелитейная промышленность, автомобилестроение, горнодобывающая промышленность [482].

На уровне экономики целью внедрения концепции I4.0 является получение максимальной выгоды от повышения качества продукции, снижения затрат и роста эффективности производства в целом [483]. Распространение цифровых технологий в промышленных цепочках создания стоимости позволяет принести значительные выгоды и повысить конкурентоспособность компаний [484]. Внедрение концепции I4.0, согласно отчету McKinsey, дает возможность сократить время простоя оборудования на 30–50%, повысить производительность труда на 15–30%, увеличить производительность продукции на 10–30% и снизить издержки на обеспечение качества продукции на 10–20% [485].

В целом, потенциальную чистую прибыль и рост капитала в ЕС от повышения уровня промышленного производства с I3.0 до I4.0 оценивают в 450 млрд евро [486]. По оценкам Accenture, рост IIoT к 2023 году добавит в мировую экономику 14,2 трлн долларов [406, 487].

Объем европейского рынка платформ, приложений и услуг для Промышленного Интернета вещей (IIoT) в 2019 году составил около 40 млрд евро. Ожидается, что этот рынок будет расти в среднем на 10% в год до 2024 года. Причем доля приложений составляет около 40% (примерно 16 млрд евро), цифровых платформ – около 8% (примерно 3 млрд евро)[18]. Машиностроительные компании в настоящее время занимают в совокупности примерно 15% от общего европейского рынка IoT [488].

---

[17] В том числе такие корпорации, как Bayer, Schneider Electric, Johnson&Johnson Vision, Groupe Renault, Johnson&Johnson, Tata Steel, Henkel, BMW Group, Procter&Gamble, Nokia, Ford Otosan, Saudi Aramco, Unilever, Siemens Industrial, Alibaba, Haier, Bosch, Hitachi и пр.

[18] Остальная часть приходится на другие услуги и области IIoT, такие как IT-безопасность, консультационные услуги, модули и датчики.

Составной частью цифровой экономики в сельскохозяйственной отрасли является концепция Agriculture 4.0 (A4.0) [489, 490]. Следует отметить, что концепция A4.0 недостаточно сформирована и во многом служит зеркальным отражением I4.0 в приложении к сельскому хозяйству [491]. A4.0 включает такие концепции, как Vertical farming, Digital agriculture, Bioeconomy, Circular agriculture, Aquaponics [492, 493, 494, 495]. Термин A4.0 используется для обозначения технологий, которые могут существенно повлиять на процесс производства, обработки, продажи и потребления продуктов питания. К ним относятся: редактирование генов, производство синтетической пищи (например, синтетического белка), нанотехнологии выращивания мяса или клеточного сельского хозяйства, биореакторы микроводорослей, дроны, IoT, робототехника и датчики, AI и ML, а также Блокчейн [496, 497, 498, 499]. Развитие парадигм IoT и Cloud позволило сформировать новые концепции в рамках A4.0, такие как [500]:

1) Precision Agriculture – PA («Точное земледелие»), которая предполагает мониторинг и реагирование на изменение цифровых сельскохозяйственных данных, собираемых датчиками [501];

2) Smart Farming – концепция, предполагающая применение информационных и коммуникационных технологий для проведения исчерпывающего анализа системы управления земледелием с учетом местоположения, накопленных цифровых данных, в том числе в режиме реального времени, а также генерирование прогнозных данных[19] [502].

Важно различать понятия Precision Agriculture (PA) и Smart Farming, поскольку PA рассматривает только изменчивость внешних (полевых) условий, в то время как Smart Farming предоставляет более комплексную концепцию, предполагающую генерирование цифровой информации для принятия управленческих и технологических решений, с учетом местоположения сельскохозяйственных активов и других данных, обогащенных исторической, оперативной и прогнозной информацией и знаниями [501].

К целям внедрения технологий A4.0 можно отнести повышение эффективности использования ресурсов, улучшение экологичности продукции и реализацию новейших тенденций, способных предоставлять потребителю подробную информацию о продуктах

[19] В рамках концепции Smart Farming парадигма IoT [503, 504] приобретает важное значение для мониторинга ресурсов путем подключения нескольких разнородных объектов смешанных молочных ферм, таких как здания, машины и оборудование, транспортные средства, крупный рогатый скот [505, 506].

питания, обеспечивая безопасность и качество конечного продукта[20]. По мнению ряда ученых, реализация концепции A4.0 способна оказать биофизическое, экономическое и социальное воздействие на продовольственную безопасность, а также на способы проектирования и эксплуатации систем сельскохозяйственного производства в мировой экономике [503].

В рамках концепции A4.0 реализуются проекты в Кастилии (Испания). Разработаны агропромышленные платформы, предназначенные для мониторинга и оптимизации управления сельскохозяйственными и животноводческими фермами. Основная цель проекта – максимизировать преимущества платформы, минимизировать ее расходы за счет эффективного управления смешанной молочной фермой[21] [206]. Новая Глобальная архитектура Edge Computing (Global Edge Computing Architecture – GECA), использована для реализации агропромышленной платформы SmartDairyTracer. Цель проекта – сформировать эталонные решения, направленные на улучшение эффективности функционирования молочной промышленности, включая оптимизацию процессов, снижение потребления воды и энергии, снижение пестицидов в сопутствующих культурах, содействие устойчивому и экологически чистому производству, мониторинг физического состояния животных и внедрение надежной системы отслеживания агропродовольственных товаров[22].

---

[20] Примером реализации концепции A4.0 является автоматизация ирригационных систем, которая позволяет измерять уровень воды в почве и управлять исполнительными механизмами для орошения [507]. Разработана система управления орошением для гидропонного точного земледелия с помощью комбинации датчиков и насосов для проведения интеллектуальных измерений кислотности и увлажненности гидропонных объектов [508, 509].

[21] Интеграция технологий в рамках концепции A4.0 сделала возможным определять местонахождение животных и следить за состоянием их здоровья в режиме реального времени. Применение методов анализа Big Data и ML облегчило диагностику, позволило связать полученные параметры с конкретными заболеваниями [510].

[22] Исследователи Университета Саламанки (Испания) и Центра цифровых инноваций (Испания) создали консорциум, объединяющий различные профили (менеджеры по животноводству, фермеры, предприятия молочной и мясной промышленности, поставщики технологий IoT, эксперты в области ИКТ, инженеры-энергетики и исследователи из научных кругов), обладающие обширным опытом в различных видах деятельности / технологиях (контроль орошения, управление энергопотреблением и оптимизация, мониторинг благополучия крупного рогатого скота, обнаружение вредителей и чумы в сельскохозяйственных культурах), чтобы задействовать всю цепочку создания добавленной стоимости молочных продуктов в процессе развертывания доступных в настоящее время инновационных технологий и решений (IoT, Distributed Ledger Technologies и AI, среди прочего), обеспечат целостное и открытое решение в форме интеллектуальной платформы на основе FIWARE [511, 512].

Для обработки этой информации и выявления болезней в животноводстве будут использоваться методы AI, предотвращения появления грибков и вредителей в сельскохозяйственных культурах (позволит сократить использование пестицидов), оптимизации потребления энергии и сокращения потребления ресурсов (умное орошение или умное управление отходами и экономика замкнутого цикла), что приведет к более устойчивому производству. Предполагается создание надежной системы отслеживания информации в системах посредством использования технологий Блокчейн, которая обеспечит защищенную от несанкционированного доступа структуру, позволяющую гарантировать безопасность и качество продукта, удостоверяющую его происхождение, и предоставит подробные данные обо всех технологических процессах[23] [513].

Следует также отметить реализацию крупных исследовательских и инновационных проектов и программ по оцифровке в рамках концепции A4.0, таких как платформа DiGISCAPE и центр продовольственной гибкости (Австралия), программа #DigitAg (Франция), программа «Интернет продуктов питания и сельского хозяйства», «Цифровые технологии» (ЕС), SmartAgriHubs (ЕС) [489]. Правительство Великобритании обязалось выделить 90 млн фунтов стерлингов (в дополнение к 160 млн фунтов предоставленных ранее) для целей внедрения новых технологий производства продуктов питания на основе концепции A4.0 [510].

Согласно исследованию McKinsey, цифровизация сельского хозяйства позволит увеличить мировой валовой внутренний продукт на 500 млрд долларов к 2030 году. По данным исследования McKinsey Center for Advanced Connectivity и McKinsey Global Institute, цифровизация сельского хозяйства даст возможность сгенерировать дополнительно от 2 до 3 трлн долларов дополнительной стоимости в мировой ВВП в течение следующего десятилетия [511].

Следующим важным компонентом цифровизации экономики является сектор энергетики. Цифровизация энергетического сектора нацелена в основном на обеспечение более эффективных, безопасных и устойчивых систем электроснабжения. Основными преимуществами цифровизации в секторе являются снижение затрат на эксплуатацию

[23] Таким образом, технологии Блокчейн могут быть использованы в рамках данной концепции в качестве механизма, с помощью которого конечные потребители могут отслеживать процессы, через которые проходит продукция по всей цепочке создания стоимости агропродовольственной отрасли, гарантируя целостность информации [513].

и техническое обслуживание, повышение эффективности, надежности и увеличение срока службы критически важных активов [101]. Концепция Smart Grid объединяет ряд технологий, потребительских решений и учитывает несколько факторов политики и регулирования, включая мониторинг, встроенную обработку и цифровую связь, что позволяет электрическим сетям быть контролируемыми (в разрезе измеряемости и визуализации), управляемыми, автоматизированными (способными к адаптации и автоматической настройке), интегрированными (совместимыми с существующими системами и способные включать разнообразные источники энергии) [514].

Следует отметить отсутствие единого определения Smart Grid, вместе с тем анализ различных подходов дает возможность охарактеризовать данную концепцию как построение прозрачной, бесперебойной двусторонней энергосети, направленной на передачу электроэнергии и информации, позволяющей энергосистеме более эффективно управлять доставкой и перераспределением электроэнергии, а потребителям гарантировать больший контроль над потребляемыми энергоресурсами. Именно повышение эффективности является основным принципом проектирования Smart Grid [515].

Smart Grid объединяет преимущества информационных технологий и передовых коммуникаций для предоставления информации в режиме реального времени и обеспечения почти мгновенного баланса спроса и предложения в электрической сети. Двусторонний обмен информацией между энергосистемой и потребителем – одно существенное различие между Smart Grid и современной энергосистемой. Таким образом, Smart Grid:

1) предоставляет потребителям лучший выбор поставщиков электроэнергии, а генерируемая сетью информация делает возможным участие потребителей в оптимизации работы системы. Smart Grid позволяет управлять спросом и реагировать на спрос путем включения интеллектуальных приборов, интеллектуальных счетчиков, микрогенерации, сохранения электроэнергии и коррекции потребительских нагрузок, а также путем предоставления потребителям информации об объемах потребления электроэнергии и актуальных тарифах. Потребителям предоставляется информация и стимулы для пересмотра структуры их потребления с целью нивелирования текущих ограничений в работе энергосистемы и повышения эффективности;

2) позволяет подключать и эксплуатировать электрогенераторы различных технологий и мощностей, а также приспособления для хранения и прерывистой генерации, тем самым значительно снижает воздействие всей системы электроснабжения на окружающую среду. Позволяет микрогенераторам работать по принципу «включай и работай», что повышает гибкость электросетей;

3) оптимизирует и эффективно управляет активами, применяя оперативную систему доставки (работающую автономно, регулируя мощности) в соответствии с потребностями;

4) работает устойчиво в условиях кибер- и физических атак, стихийных бедствий и доставляет электроэнергию потребителям с повышенным уровнем безопасности и надежности;

5) открывает доступ к новым рынкам посредством увеличения совокупного предложения, путей передачи, вспомогательных услуг и инициатив. Растет роль потребителей в цепочке поставок энергии, они превращаются из чистых потребителей электроэнергии – в частично потребителей и частично производителей prosumer.

Воздействие цифровизации на различные части цепочки создания стоимости электроэнергии имеет следующие особенности [101].

1. Преимущества в управлении генерирующими активами в основном сосредоточены на оптимизации технического обслуживания оборудования, топлива и запасных частей. Используемые технологии будут включать дистанционное зондирование и цифровые мониторы, новые системы управления с автоматическим прогнозированием и дистанционным обслуживанием / контролем, возможно, связанные с прогнозируемыми рыночными условиями, расширенный интеллект – для принятия решений и ML – с целью улучшения краткосрочных прогнозов для балансирования и торговли.

2. Цифровизация может повысить эффективность принятия управленческих решений в торговле и при планировании генерации за счет использования стратегий, основанных на Big Data, новых моделях управления рисками, новых торговых продуктах и алгоритме торговли, включая оптимизацию краткосрочных целей.

3. Снижение потерь, снижение трудозатрат и прогнозное обслуживание в сетях передачи и распределения благодаря дистанционному мониторингу в реальном времени, данным датчиков в реальном времени, помогающим в прогнозировании, в центрах данных, собирающих данные интеллектуальных счетчиков, и расширенному интеллекту для управления работой сети. Кроме того, цифровизация

и интеллектуальное переключение в сетях с более низким напряжением могут способствовать отложенным / исключенным инвестициям в сеть и переходу к активному управлению распределительными сетями. Новые регулирующие подходы могут появиться на основе общих данных, которые сужают информационную асимметрию между компаниями и регулирующими органами.

4. Цифровизация розничного сектора. Установление прямых отношений с клиентами позволит сформировать предложение новых продуктов и услуг, снизить цены, осуществить системную дифференциацию клиентов с помощью цифрового маркетинга, проводить электронное выставление счетов и взимание платы за доступ к сети, предоставить дополнительные услуги, организовать одноранговую торговлю. Другими словами, цифровизация позволит предлагать более персонализированные услуги и тарифы.

Важным элементом концепции Smart Grid является Cloud Computering, обеспечивающее удаленное хранилище данных, автоматические обновления, сокращение расходов на обслуживание IT-систем за счет экономии энергии, финансовых ресурсов и рабочей силы.

Прорабатываются возможности интеграции технологий Блокчейн[24] в концепции Smart Grid. Блокчейн позволит технологиям обеспечить устойчивую тенденцию децентрализации [516], концепции которой имеют несколько схожих наименований, таких как «микросеть» (microgrid), «энергетический хаб» (energy hub) [517], «наносеть» (nanogrid) [518], «мезосеть» (mesogrid), «энергетический Интернет» (energy Internet), «коммунальная энергосеть» (community energy network), «социальная энергосеть» (social energy network), «одноранговая энергосеть» (peer-to-peer (P2P) energy network) и «виртуальная электростанция» (virtual power plan) [517].

Следует выделять ряд проектов интеграции технологий Блокчейн в Smart Grid на уровне коммунального хозяйства в отдельных районах г. Нью-Йорка (США) [519, 520], г. Перта (Австралия) [521]. Проводятся испытания внедрения P2P платформ Piclo (Великобритания) [522], Vandebron (Нидерланды) [523]. Прогнозы интеграции технологии Блокчейн в концепцию Smart Grid расходятся: так, по данным аналитической компании INFOHOLIC Research LLP, совокупный объем используемых в отрасли Блокчейн-продуктов

[24] Блокчейн предоставляет возможность формирования децентрализованной базы данных для определения владельца энергии и управляет множеством торговых соглашений между потребителями и продавцами [519].

к 2024 году превысит 3,5 млрд долларов, а согласно прогнозу Zion Market Research, он достигнет 12 млрд долларов[25].

В европейском регионе лидером в имплементации технологий Smart Grid является Соединенное Королевство. В Великобритании реализуется программа внедрения интеллектуальных счетчиков (Smart Meter Implementation Programme), в соответствии с которой в 2020 году установлено 53 млн интеллектуальных счетчиков газа и электроэнергии [487]. В рамках Третьего энергетического пакета ЕС (Директивы 2009/72/ЕС) предусматривается внедрение в странах Европейского союза интеллектуальных счетчиков (около 200 млн интеллектуальных счетчиков электроэнергии и 45 млн газовых счетчиков). Китай также начал внедрять концепцию Smart Grid в 2009 году [21, 524].

Согласно данным Международного энергетического агентства (IEA), внедрение технологий Smart Grid, децентрализация сетей позволят сэкономить к 2040 году дополнительных вложений в новую электроэнергетическую инфраструктуру, включая новые мощности по производству электроэнергии, передаче и распределению, в размере 270 млрд долларов [101]. С учетом современных технологий и ресурсов, по оценкам IEA, 1 млрд домашних хозяйств и 11 млрд интеллектуальных устройств могут обеспечить удаленный мониторинг и управление энергопотреблением.

На уровне управления городской инфраструктурой статус цифровой парадигмы приобрел концепт Smart City, в том числе благодаря развитию технологий IoT, генерирующих большой объем данных, требующих скоростной обработки в режиме реального времени [525]. Концепция Smart City существует с середины 1990-х годов [175, 526]. Вместе с тем концептуализация Smart City развивается, и согласованное определение в настоящее время отсутствует [527]. Представляется, что в самом широком понимании, концепция Smart City предполагает синергию цифровых технологий и управления городской инфраструктурой с целью оптимизации затрат и обеспечения высокого уровня благосостояния горожан[26]. В данном контексте реализация концепции Smart City требует

[25] ТОП-10 сфер применения технологии Блокчейн, не связанных с криптоиндустрией. – Режим доступа: https://whattonews.ru/top-10-sfer-primenenija-tehnologii-blokchejn-ne-svjazannyh-s-kriptoindustriej/. – Дата доступа: 25.09.2021.

[26] Согласно прогнозам ООН, к 2050 году 86% развитых стран и 64% развивающихся стран будут урбанизированы [526, 528].

использования современных технологий, включая 5G[27], AI, для формирования сетевой инфраструктуры как совместимой экосистемы платформы, имеющей такие характеристики, как открытость, инклюзивность, прозрачность, и защиту данных [175]. Технологии, составляющие Smart City, включают в себя Smart Grid, устройства и датчики IoT, услуги сетевых информационных технологий, телекоммуникационные технологии, технологии проводной и беспроводной инфраструктуры, программное обеспечение и т. д.[28] В мировой практике условно выделяются три уровня развития (три поколения) концепции Smart City. Первое поколение таких городов (Smart City 1.0) предполагает имплементацию отдельных решений на базе платформ информационно-телекоммуникационных технологий (ИКТ); в рамках концепции Smart City 2.0 применяются цифровые модели и общегородские платформы сервисов. Концепция Smart City 3.0 предполагает формирование высокоинтеллектуального интегрированного города, который характеризуется следующими параметрами [529]:

а) объединением технологий, стимулирующих развитие социальной интеграции и предпринимательства;

б) внедрением передовых цифровых сервисов (цифровая трансформация секторов экономики) и формированием полностью интегрированной интеллектуальной инфраструктуры, позволяющей в режиме реального времени осуществлять сбор и аналитику Big Data, реализовывать управление всеми процессами во всех областях инфраструктуры;

в) переориентацией городских процессов относительно потоков данных: единая экосистема способствует вовлечению граждан, делая их активными участниками развития города.

---

[27] 5G связь, предназначенная для обеспечения эффективного соединения между интеллектуальными устройствами и приложениями, создает взрывной рост трафика данных мобильных пользователей в широком спектре новых инновационных услуг. Основные технологические отличия 5G по сравнению с предыдущими стандартами передачи данных: а) более высокая скорость передачи данных; б) более высокая плотность мобильного трафика; в) более высокая надежность связи; г) поддержка более высоких пользовательских скоростей; д) меньшее время задержки отклика сети: е) возможность одновременного подключения большого массива устройств; ж) возможность снижения мощности сигнала при поддержке IoT [531].

[28] Ключевые компоненты Smart City: Smart manufacturing, Wi-Fi, Digital citizens, Smart transportation, Smart security, Smart home, Open data, Smart farming, Smart buildings, Smart grid, Smart health, Smart government, – могут использовать различные комбинации этих компонентов в зависимости от потребностей городов [532, 533].

Как отмечает Занелла, целью реализации Smart City является повышение качества обслуживания граждан при одновременном снижении общих эксплуатационных расходов государственного управления [530]. Мерсел – Ллакуна, Коломер – Ллинас, Мелендес – Ллинас расширяют целеполагание данной концепции, обосновывая необходимость предоставления городскими властями «более эффективных услуг гражданам, осуществление контроля и оптимизации существующей инфраструктуры, расширение сотрудничества между различными субъектами экономической деятельности и поощрение инновационных бизнес-моделей как в частном, так и в государственном секторе» [534].

Следует отметить ряд проектов концепции Smart City в различных странах. Так, в 2014 году Правительством Великобритании взяты обязательства осуществить финансирование проекта стоимостью 24 млн фунтов стерлингов в г. Глазго, а также выделить 3 млн фунтов городам Лондону, Бристолю и Питерборо [535]. Примером реализации концепции Smart City является проект «Амстердам Smart City», который представляет собой конвергенцию и синергию предприятий, органов власти и исследовательских институтов с целью преобразования данного региона в Smart City, обеспечивающий высокий уровень жизни, развитую рабочую среду, мобильность, доступность государственных услуг и открытость данных [536]. Согласно рейтингу Smart City Government, разработанному компанией Eden Strategy Institute, по состоянию на 2020–2021 годы лидерами в реализации данной концепции являются Сингапур, Сеул, Лондон, Барселона, Хельсинки и Нью-Йорк[29].

Согласно исследовательским прогнозам, объем рынка экономики Smart City к 2025 году достигнет 3 трлн долларов [537, 538]. Компания IHS Technology прогнозирует увеличение количества Smart City в мире в четыре раза с 2013 по 2025 год (с 21 до 88) [528, 539].

В последние годы объединение технологий транспортных средств и сетевых коммуникаций продолжает расширять границы, формируя Intellectual Transport Systems (ITS). Концепция ITS предполагает использование расширенного функционала автомобиля для обработки в режиме реального времени и передачи сигналов, анализа и прогнозирования поведения и условий движения с помощью различных интеллектуальных цифровых устройств [211].

[29] Celebrating the world's leading Smart city. – Режим доступа: governments https://www.smartcitygovt.com. – Дата доступа: 15.02.2022.

Концепция специальных автомобильных сетей получила название – VANET (Vehicular Ad hoc Networks)[30]. Основная цель сети – обеспечить безопасность и эффективность движения с точки зрения сокращения времени движения, финансовых затрат и выбросов загрязняющих веществ [540]. Интегрируя инфраструктуру, транспортные средства и дороги, ITS позволяет избежать ДТП[31], сократить время в пути, уменьшить транспортные заторы, обеспечить дополнительный контроль энергопотребления, сократить загрязнение окружающей среды[32].

Дополнительным интегрируемым элементом ITS является страхование ответственности на основе времени использования транспортных средств (Usage-based insurance), которое позволяет собирать данные о вождении и хранить их в Блокчейн [541]. Данная система сокращает страховые платежи для владельцев транспортных средств, отправляя цифровые данные о вождении для оценки его стиля, влияющего на безопасность.

По оценкам McKinsey, объем инвестиций в сектор интеллектуальных транспортных систем 2010–2020 годы составил почти 330 млрд долларов [545].

Финансовая сфера цифровизации экономики является одной из самых адаптивных к цифровым инновациям. При этом экономическая теория подчеркивает устойчивую связь между финансовым и экономическим развитием государства [546]. Шумпетер выдвинул теорию, согласно которой предпринимательство и технологические инновации могут эффективно функционировать и генерировать экономический рост только при поддержке кредитного или финансового рынка поскольку «…предприниматель не накапливает для того, чтобы получить необходимые ему средства, и не аккумулирует никаких товаров перед тем, как начать производить» [7]. Связь между финансовым развитием и экономическим ростом аргументированно

---

[30] VANET имеют разнообразные приложения обмена информацией между транспортными средствами и инфраструктурой ITS посредством протоколов связи, таких как транспортное средство – транспортное средство (vehicle-to-vehicle V2V), транспортное средство – инфраструктура vehicle-to-(roadside) infrastructure (V2I) и транспортное средство – сеть vehicle- to-network (V2N) или связь транспортных средств со всеми объектами vehicle-to-everything (V2X) [541, 542].

[31] Согласно отчету Министерства транспорта США (DoT), системы ITS позволяют предотвратить 82% аварий [543].

[32] По оценкам McKinsey Global Institute, синергия технологий в области «умного автомобилестроения», здравоохранения, промышленного производства и розничной торговли позволит увеличить мировой ВВП к 2030 году на 1,2 трлн долларов [544].

установлена в работах Голдсмита, Кинга и Левина, Зервоса [547, 548]. Так, Голдсмит доказывает, что коэффициент финансовых взаимосвязей[33] увеличивается в ходе финансового развития, но после достижения определенной стадии развития – когда коэффициент близок к единице или немного превышает ее – изменения становятся небольшими, за исключением радикальных разрывов в непрерывности из-за войн и валютных реформ [549].

Вместе с тем, как отметили Бек, Чен, Лиин, Сонг, финансовые инновации ведут к более хрупкой и уязвимой финансовой системе, что, в свою очередь, препятствует экономическому росту [550, 551].

Маккиннон и Шоу выделили следующие причины, по которым неразвитые финансовые системы могут препятствовать росту экономики: ограничение объема сбережений для мобилизации инвесторами, а также нехватка самих финансовых посредников для перенаправления денежных ресурсов в наиболее продуктивные сферы [552, 553, 554]. Давей, Энци, Джен отмечают, что «…структура финансирования должна соответствовать структуре экономики. Соответствующие отношения напрямую отражаются в балансе структурного спроса и предложения» [546]. Левин описал влияние финансов на экономический рост посредством упрощения обмена товарами и услугами, генерирования информации, мониторинга инвестиций и осуществления корпоративного контроля, диверсификации и управления рисками [555]. Как отметили Берне и Плуф [549], «…финансовые инновации оптимизируют процесс финансового посредничества и, в свою очередь, стимулируют экономический рост». Финансовые инновации повышают эффективность распределения сберегательного капитала в инвестиционный капитал, а также увеличивают ликвидность на рынках. В записке, опубликованной МВФ в 2013 году, говорится, что «секьюритизация[34] может помочь

[33] Коэффициент финансовых взаимосвязей. Это, вероятно, самая широкая поддающаяся количественной оценке концепция, которую можно использовать для характеристики финансовой структуры и развития в национальном масштабе. Он определяется как отношение совокупной стоимости нематериальных активов к материальным активам в объединенном национальном балансе и измеряет плотность финансового покрытия экономики. Изменения коэффициента финансовой взаимосвязи также отражают относительные темпы роста финансовых активов и материального благосостояния. Коэффициент финансовой взаимосвязи между потоками дополняется соотношением денежного и неденежного (бартерного и вмененного) дохода.

[34] Создание ценных бумаг из портфеля существующих активов или будущей дебиторской задолженности, которые передаются в юридическую собственность, или контроль инвесторов через специального посредника, созданного для этой цели, – «структуру специального назначения» (SPV) или «компанию специального назначения» (SPE) [556].

эмитентам и инвесторам диверсифицировать и передавать риски между различными классами активов, географическими регионами, отраслями, инструментами и кредитным риском. Превращая пул неликвидных активов в торгуемые ценные бумаги, секьюритизация также представляет собой потенциально ценный инструмент для помощи в возобновлении кредитного потока для достойных заемщиков» [556, 557].

Цифровая трансформация финансового сектора привела к цифровизации бизнес-моделей и процессов, создала новые продукты и услуги. Юнгер и Мицнер отмечают тенденции роста цифровых консультативных и торговых систем, внедрение AI и ML, одноранговое кредитования (P2P), crowdfunding, мобильных платежных систем и новых денежных возможностей с различными цифровыми формами денег [558]. Скардови выделил следующие перспективные направления цифровизации основных элементов финансового сектора: платежные системы, сбережения и инвестиции, проектное финансирование, депозитные и кредитные услуги, инвестиционный и корпоративный банкинг, страхование и перестрахование, управление рисками [559]. Цифровые технологии позволяют автоматизировать широкий спектр финансовой деятельности, предоставляя новые экономически эффективные продукты в некоторых сегментах финансового сектора [560].

По мере развития цифровой экономики произошло частичное замещение функционала традиционных крупных финансовых институтов новыми финансовыми институтами и механизмами, концептуально объединенными термином FinTech, который предполагает конвергенцию традиционных финансовых услуг с мобильными услугами, услугами социальных сетей, агрегированием и обработкой Big Data, Cloud Computing [561].

Следует отметить отсутствие в экономической литературе единого подхода к определению FinTech. С учетом современных тенденций формирования и развития FinTech, основных характеристик данной концепции, ее можно определить как конвергенцию цифровых технологий и финансовых услуг, направленную на оптимизацию экономической деятельности как поставщиков, так и потребителей финансовых услуг, посредством сокращения себестоимости и улучшения качественных характеристик оказываемых услуг, а также на разработку инновационных механизмов, инструментов, продуктов и бизнес-процессов. С точки зрения

институционализма FinTech представляет собой системные отношения, по поводу предоставления высокотехнологических цифровых финансовых услуг, и финансовых (и посреднических) институтов, обслуживающих данные отношения, включая цифровые платформы и приложения, банковские организации, финансовые и страховые компании, биржевые площадки, телекоммуникационные и продуктовые IT-компании.

FinTech-предприятия предлагают гибкие модели обслуживания, сфокусированные на контекстных продуктах, адаптированных к индивидуальным профилям клиентов[35][562].

Среди причин стремительного развития FinTech в современной экономике выделяют следующие [546, 563]:

1) недостатки традиционного финансового рынка и избыточное государственное регулирование данной отрасли;

2) общественное недоверие к традиционной индустрии финансовых услуг;

3) коммерциализация цифровых технологий и проникновение на рынок финансовых услуг Интернета и мобильных телефонов;

4) наличие отдельных лакун рынка финансовых услуг, которые не являются привлекательными для традиционных банковских институтов с точки зрения максимизации прибыли (например, МСП)[36]. При этом цифровые платформы предлагают широкий спектр продуктов, специально адаптированных к потребностям МСП, включая финансирование для пополнения оборотного капитала, торговое финансирование, финансирование расчетов и онлайн-торговли, в том числе онлайновых цепочек поставок [564].

5) международная политика в сфере финансовой доступности (инклюзивности). По оценкам Международной финансовой корпорации, в развивающихся странах финансово исключенные МСП сталкиваются со значительным кредитным разрывом, превышающим

---

[35] Расширение возможностей бизнес-экспертов в области аналитики, а также умелое использование данных сегментации и прогнозной аналитики позволяет доставлять пакеты специализированных продуктов по нескольким каналам доставки (Интернет, мобильные устройства, точки продаж и т. д.).

[36] Небольшой объем транзакций и низкая прибыльность финансовых услуг, оказываемых предприятиям МСП, снижают экономическую мотивацию банков по обслуживанию такого рода предприятий. Применение Fintech технологии больших данных расширяет эффективную границу оказания финансовых услуг, тем самым позволяет снизить транзакционные издержки, связанные с необходимостью обработки каждого отдельного бизнес-запроса на предоставление финансирования, оценить риски.

2,1 трлн долларов США[37] [565]. По оценкам Всемирного банка Global Findex, около 1,7 млрд людей старше 18 лет в мире не имеют банковских счетов. Большая часть этого населения проживает в развивающихся странах, а около половины сосредоточено в семи странах: Бангладеш, Китае, Индии, Индонезии, Мексике, Нигерии и Пакистане[38] [566, 567].

Использование термина «финансовая доступность» (Financial Inclusion) относится к двум различным аспектам финансовой доступности: «доступ» к финансовым продуктам и «использование», т. е. способы, которыми клиенты используют предоставляемые услуги. Центр финансового вовлечения Accion определяет «финансовую доступность» как состояние, в котором все люди, которые могут их использовать, имеют доступ к полному набору качественных финансовых услуг, предоставляемых по доступным ценам, удобным способом и с достоинством для клиентов [568]. Характеристиками финансовой доступности являются: 1) равномерная доступность финансовых услуг; 2) регулярное использование; 3) хорошее качество финансовых услуг; 4) потенциал для повышения благосостояния. Эта проблема может иметь отношение к любой части населения, независимо от социального статуса или дохода, и к любой стране, независимо от ее статуса развития [569].

Ряд исследований показал, что доступ к финансам снижает уровень бедности, позволяет увеличить занятость и доходы в регионах с низким уровнем дохода [570, 571, 572]. Отмечается прямая корреляция между уровнем человеческого развития и финансовой доступностью, положительное влияние финансовой интеграции на макроэкономические показатели: экономическую стабильность, совокупное потребление [573, 574, 575]. Отсутствие доступа к финансовым услугам, как показал ряд исследований, может привести к ловушкам бедности и социальному неравенству [569, 571, 576].

---

[37] Как показало исследование, проведенное CARE International и Accenture, включение неохваченных банками МСП в клиентскую базу банковского сектора может принести банкам дополнительный годовой доход в размере около 270 млрд долларов США. Наибольший потенциал доходов оценивается в Азиатско-Тихоокеанском регионе в 95 млрд долларов США.

[38] Африка является регионом с наименьшим количеством банков в мире, и, по оценкам, 80% ее населения не имеют доступа к официальным банковским услугам. В Азии средний процент владения банковским счетом и дебетовой картой составляет 53,2% и 32% соответственно; в Латинской Америке – 46,7% и 31,2%; в развивающейся Европе – 58,1% и 43,2%.

С целью решения проблемы финансовой доступности в 2010 году было основано Глобальное партнерство по финансовой доступности (Global Partnership for Financial Inclusion, GPFI), в 2015 году Группа Всемирного банка, МВФ и партнеры из государственного и частного секторов приняли измеримые обязательства по достижению всеобщего доступа к финансам к 2020 году (программа UFA2020)[39] [577]. Продвижение технологических инструментов для улучшения доступности финансовых услуг является одним из направлений Целей Организации Объединенных Наций по устойчивому развитию, принятых Организацией ООН в 2015 году.

Преимуществами FinTech, по сравнению с традиционными финансовыми институтами, являются [178]:

1) меньший объем обязательств по соблюдению регуляторных требований;

2) более низкие эксплуатационные расходы, поскольку FinTech-предприятия не участвуют в банковском обслуживании с частичным резервированием и могут осуществлять трансграничные переводы, не полагаясь на межбанковский клиринг. У FinTech-компаний отсутствует необходимость создания и поддержания физических активов (филиальной сети) [559];

3) на FinTech-компании не распространяются требования к капиталу, установленные международным банковским регулированием (GPFI);

4) в отличие от FinTech-компаний, банки имеют массивные устаревшие ИТ-системы и бизнес-процессы, которые затрудняют внедрение новых технологий в их инфраструктуру.

По мнению управляющего Банка Англии Карни [578], FinTech увеличивает возможности экономических агентов, в том числе:

а) для потребителей расширяется выбор, услуги становятся более целенаправленными и по более низким ценам;

б) МСП получают доступ к новым кредитам;

в) банки повышают продуктивность деятельности, снижают транзакционные издержки, повышают эффективность капитала и операционную устойчивость;

---

[39] В рамках инициативы «Универсальный доступ к финансовым услугам 2020» Группа Всемирного банка – Всемирный банк и IFC – взяла на себя обязательство предоставить 1 млрд человек доступ к операционному счету посредством целевых мероприятий (UFA2020 Overview: Universal Financial Access by 2020. – Режим доступа: https://www.worldbank.org/en/topic/financialinclusion/brief/achieving-universal-financial-access-by-2020. – Дата доступа: 1.10.2018).

г) финансовая система государства становится более устойчивой, более разнообразной, комплексной и емкой;

д) повышается доступность финансовых услуг, улучшается информированность и финансовая грамотность населения.

Более того, для инвесторов FinTech-компании предоставляют возможность снижать кредитные риски благодаря механизмам резервных фондов или кредитным гарантиям. Резервы функционируют как частная схема страховпания вкладов[40]. FinTech оценивает кредитоспособность, используя более эффективные метрики, позволяя кредиторам выбирать желаемый профиль риска (доходности) и соответствующий кредитный портфель[41]. Это дает возможность предоставлять кредитные финансовые услуги по фиксированным ставкам, даже в условиях роста процентных ставок на рынке [559]. FinTech-платформы P2P-кредитования обеспечивают высокую скорость обработки запросов благодаря использованию технологий Big Data, Cloud Computing и AI [564].

К недостаткам FinTech можно отнести следующие аспекты [96]:

1) сложность принятия потребителями новых систем FinTech, по причине ограниченности знаний о возможностях мобильных платежей;

2) сомнения потребителей в надежности цифровых решений;

3) сложность самих цифровых платформ;

4) обеспечение конфиденциальности и безопасности.

В экономической литературе выделяются следующие подходы к классификации FinTech.

1. По критериям предоставляемых сервисов и услуг [579]:

а) платежные;

б) страховые;

в) управления рисками;

г) однорангового (P2P) кредитования;

---

[40] Платформы откладывают часть сборов за выдачу кредита, уплачиваемых заемщиками в резервный пул, что является общим для всего портфеля, и поэтому риск инвестора распределяется по всей кредитной книге. Денежные средства хранятся в трасте и отделены от активов бизнеса. Так, в Соединенном Королевстве большинство крупных платформ имеют резервные фонды, предназначенные для компенсации инвесторам, подверженным дефолтам по кредитам.

[41] Кредитный андеррайтинг является важной частью P2P-кредитования. Чтобы установить кредитоспособность заемщика, большинство платформ используют данные кредитных бюро, кредитные оценки, отражающие историю финансового поведения в прошлом, и другие альтернативные источники данных. Оценка кредитного риска остается сложной задачей на рынках, не имеющих бюро кредитных историй или платформы которых ориентированы на новые сегменты клиентов без адекватной кредитной истории.

д) аутентификации;

е) фонды денежного рынка (MMF).

2. По критериям составляющих элементов инфраструктуры цифровых платежных сервисов [580]:

а) цифровые кошельки (приложения, используемые для осуществления платежей, представляющие собой оцифрованные версии кредитных карт);

б) мобильные одноранговые (P2P) платежи (позволяют частным лицам осуществлять платежи физическим и юридическим лицам, замещая такие платежные инструменты, как наличные денежные средства, чеки или пластиковые карты. Некоторые из этих сервисов встроены в функционал социальных сетей);

в) точки продаж (POS) (цифровые решения для устройств и программ, которые обеспечивают цифровое движение денежных средств, отслеживают запасы, генерируют отчеты о продажах, а также предоставляют аналитику);

г) монетизация цифровых данных – значительный объем данных, передаваемых через провайдеров платежей, дает представление о структуре потребительских расходов, макротрендах и потенциале для выявления и предотвращения мошенничества.

3. По критериям цифрового предоставления банковских услуг [581]:

а) обеспечение функционирования платформ для онлайн-платежей;

б) услуги мобильного банкинга;

в) услуги по переводу денег;

г) обеспечение функционирования точек продаж посредством соответствующего цифрового оборудования;

д) обеспечение функционирования мобильных кошельков;

е) предоставление банковского обслуживания;

ж) обеспечение функционирования мобильных денег, интегрированных с инфраструктурой систем межбанковских платежей.

4. По критериям предоставления услуг алгоритмической торговли [546]:

а) компании, которые предлагают высокоавтоматизированное управление и консалтинг[42];

[42] Услуги с высокой добавленной стоимостью по распределению портфеля и управлению денежными средствами при низких затратах на основе автоматического анализа, при котором автоматизация персонализированного инвестиционного портфеля основана на потребностях клиента с учетом общего риска (доходности).

б) компании, которые сосредоточены на создании и передаче инвестиционных стратегий и портфелей другим инвесторами, а также предоставлении консалтинговых услуг;

в) компании, непосредственно предоставляющие услуги алгоритмической торговли[43].

5. По критериям осуществляемых финансовых операций [582]:

а) кредитование (предоставление цифровых решений в форме платформ, на которых клиенты могут получать финансовые ресурсы напрямую от других клиентов или финансовых учреждений (например, краудфандинг, мгновенное кредитование);

б) инвестирование (предоставление цифровых решений для улучшения инвестиционных возможностей клиентов (например, роботоконсультирование, инвестиционное посредничество);

в) страхование (предоставление новых моделей страхования);

г) проведение платежей (предоставление платежных решений (например, мобильные платежи, криптовалюта));

д) предоставление услуг расчетного счета (решений для управления счетами и выставления счетов (например, интегрированные решения для цифрового учета));

е) осуществление межпродуктового сервиса (разработка приложений, которые поддерживают взаимодействие клиентов со своими контрагентами, такими как банки и страховые компании (например, идентификация видео, переключение банков));

ж) предоставление API и инфраструктуры в качестве цифровых интерфейсов для других компаний и клиентов (разработка цифровых интерфейсов, которые позволяют другим компаниям предоставлять решения для клиентов или связываться с другими компаниями (например, интегрированной логистикой)).

6. По критерию привязки к существующей платежной инфраструктуре [583]:

а) «оверлейные системы» (например, Google Pay, Apple Pay и PayPal), которые разработаны на основе существующих платежных инфраструктур для клиринга и расчетов, включая кредитные карты или системы быстрых розничных платежей;

б) «проприетарные системы» (например, Alipay и WePay), которые являются более замкнутыми по своей природе, клиринговые

---

[43] Услуги предоставляются даже розничным инвесторам и позволяют создавать, тестировать и выполнять инвестиционные алгоритмы в их интересах, даже в условиях ограниченных технических знаний и отсутствия собственной клиентской IT-инфраструктуры.

и расчетные транзакции в рамках инфраструктур, разработанных и управляемых самими технологическими фирмами.

В целом, следует отметить следующие тенденции развития FinTech в мировой экономике:

1) расширение взаимодействия по линии традиционные банковские организации – компании FinTech. Так, банки увеличивают объемы предоставления кредитов через онлайн-платформы, что стимулирует финансовую доступность[44]. Тем не менее, по мере углубления этого сотрудничества и значительного увеличения объемов кредитования, повышенное внимание регулирующих органов будет уделяться данному сегменту [552, 584];

2) расширение использования электронных платежей по таким направлениям, как [585]:

а) рост оборотов банковских (финансовых) услуг, встроенных в бизнес-модели небанковских организаций (Banking-as-a-Service, BaaS). Данная услуга, которую также называют «встроенным финансированием», создает возможность для любой технологической компании стать финансово-технологической[45];

б) усиление вмешательства государства в сектор FinTech. Формирование нормативно-правовой базы создаст условия для расширения внедрения новых услуг и продуктов на финансовом рынке, позволит уменьшить ассоциации инновационных финансовых инструментов с мошенническими операциями, снизит риски для потенциальных клиентов, создаст условия для развития платежной экосистемы;

в) переоценка компаниями рисков, связанных с использованием услуг и продуктов сторонних поставщиков, уменьшение зависимости

---

[44] Вместе с тем, как показали исследования консалтинговой компании BCG в отношении банков, осуществляющих операции исключительно в цифровом формате, только 13 из 249 таких банков прибыльны. При этом 10 из них находятся в Азиатско-Тихоокеанском регионе, а 3 – в Европе, в Америке прибыльных цифровых банков не оказалось. В число прибыльных цифровых банков вошел российский Тинькофф банк (Winning the Digital Banking Battle in Asia-Pacific. – Режим доступа: https://mkt-bcg-com-public-pdfs.s3.amazonaws.com/prod/digital-banking-asia-pacific.pdf. – Дата доступа: 23.08.2021).

[45] Крупные технологические компании с существующими продуктами и услугами диверсифицируют свои интересы в сфере платежей и сектора финансовых услуг. Будучи хорошо известными и пользующимися доверием брендами с большой пользовательской базой и сильным финансовым положением, технические специалисты в области финансовых услуг могут быстро расширить свою деятельность. Эти игроки также могут использовать и, в свою очередь, извлекать выгоду из агрегированных данных о поведении и предпочтениях потребителей, собранных в рамках их существующих услуг и продуктов.

от посредников, повышение уровня контроля над транзакциями и общей безопасности средств;

г) расширенное использование биометрии для подтверждения личности покупателя и одобрения. Для потребителей возможность подтверждать покупки по лицу или отпечаткам пальцев позволит отказаться от необходимости ввода паролей, поскольку все используемые платежные сервисы могут быть защищены с помощью одной персональной функции. Это также ускорит весь процесс, более того, это обеспечивает дополнительный уровень безопасности, поскольку мошенникам труднее скопировать персональные данные;

д) повышение гибкости платежей. Крупные игроки рынка, такие как PayPal и Chase, предложили отсрочку платежа по схеме «покупай сейчас, плати потом», которая предоставляет возможность оплачивать покупки в течение определенного периода времени с нулевой процентной ставкой и фиксированной ставкой за ежемесячные платежи. Концепция гибкости включает не только варианты отложенных платежей, но и появление новых платежных платформ;

3) поступательный переход к внедрению цифровых валют как важный шаг в развитии платежных систем и инструментов. Децентрализованные платежные системы предотвращают утечку данных, простои и зависимость от посредников [583]. Блокчейн может обрабатывать транзакции мгновенно, смарт-контракты обеспечат большую прозрачность, а деньги станут программируемыми, предотвращая мошенничество и уклонение от уплаты налогов.

Представляется целесообразным рассмотреть FinTech в разрезе ключевых цифровых концептов, определяющих основные направления развития финансовых технологий, включая:

1) новый FinTech-инструментарий для кредитно-инвестиционной и проектной деятельности (Crowdfunding, P2P-кредитование);

2) внедрение FinTech в традиционные финансовые сегменты и их трансформация (алгоритмическая торговля);

3) использование мобильного функционала FinTech (специализированного ПО для мобильных телефонов) для трансформации банковской сферы и платежных систем (мобильный банкинг, мобильные деньги и мобильные платежи);

4) внедрение FinTech в сектор страхования (IsurTech);

5) реализация функционала FinTech для трансформации государственных платежных систем (CBDC, RTGS);

6) внедрение функционала FinTech для формирования банковских цифровых платформ и цифровизации отдельных операций (RegTech);

7) внедрение функционала FinTech для формирования биржевых цифровых платформ;

8) развитие криптовалютного рынка и соответствующей цифровой инфраструктуры.

Важнейшим компонентом FinTech является концепция Crowdfunding. Важно отметить отсутствие единого определения данной концепции финансирования. Crowdfunding как механизм финансирования обеспечивает привлечение заемных средств с использованием онлайн-платформы [70]. Таким образом, Crowdfunding превращает традиционного финансового посредника в веб-платформу, которая снижает затраты и расширяет базу инвесторов [586, 587]. При этом Crowdfunding-платформы не являются финансовыми посредниками, поскольку они не участвуют в принятии инвестиционных решений[46] [588].

Важно отметить, что Crowdfunding является FinTech-институтом цифровой экономики, который представляет новую систему отношений между кредиторами и заемщиками, опосредованную цифровыми платформами.

К преимуществу механизма Crowdfunding следует отнести сокращение ограничений во внешнем финансировании (у заемщиков нет необходимости предоставлять соответствующее обеспечение по кредитам) [118]. Кроме того, механизм Crowdfunding дает возможность заемщикам [178]:

1) получить более дешевое внешнее финансирование;

2) привлечь социальное внимание;

3) получить обратную связь по предлагаемому продукту или услуге от потребителей.

Представляется целесообразным классифицировать Crowdfunding-платформы следующим образом [178].

---

[46] Некоторые платформы Crowdfunding-акций объединяют средства толпы в инвестиционный инструмент и представляют интересы толпы по отношению к компании, которая получает финансирование. Но даже в этом случае платформа не занимается управлением портфелем, и поэтому Crowdfunding-платформы следует рассматривать как посредники или онлайн-рынки. Плата, которую взимают платные инвестиционные платформы за свои услуги, может значительно варьироваться. В то время как компании обычно платят комиссию в размере 5–10% от собранной суммы, некоторые платформы взимают дополнительную фиксированную предоплату. Другие платформы также взимают плату с инвесторов. Эти сборы являются либо фиксированными, либо процентами от вложенной суммы. В некоторых случаях с инвесторов взимается комиссия в зависимости от их прибыли.

1. По критерию назначения привлекаемого финансирования:

а) платформы общего назначения (Crowdfunding для любой области интересов);

б) тематические платформы (ориентированы на Crowdfunding для проектов в определенной области или секторе).

2. По критерию используемых механизмов финансирования:

а) платформы, регулирующие уровень залога;

б) платформы, регулирующие минимальные суммы инвестиций;

в) платформы, использующие принцип финансирования «все или ничего» (all or nothing), которые позволяют сторонникам проекта получать финансирование только в том случае, если кампания аккумулирует всю заявленную сумму[47];

г) платформы, использующие принцип финансирования «сохранять все» (keep it all), позволяют участникам проекта получать любую собранную сумму.

3. По критерию используемой инвестиционной модели [118, 178, 558]:

а) неинвестционные модели:

– донорство (Donation Crowdfunding) – метод сбора средств на благотворительные, социальные или политические кампании. Участники проекта не получают материальных благ;

– наградной Crowdfunding (Reward Crowdfunding) – метод финансирования, при котором любой участник, вносящий денежные средства, получает вознаграждение в форме товаров или услуг, которые владелец проекта реализует на рынке;

б) инвестиционные модели:

– одноранговое (бизнес) кредитование (Peer-to-peer (business) lending), долговое финансирование. Кредиторы или инвесторы предоставляют деньги для поддержки проекта или бизнеса. Кредиторы предлагают кредит в ожидании получения своего основного долга и процентов по нему в заранее установленный срок. Платформы онлайн-кредитования P2P представляют собой конвергенцию P2P-кредитования и Crowdfunding, обеспечиваемую интернет-платформой[48];

– долевой Crowdfunding (Equity Crowdfunding), предоставление средств в форме эмиссии акций (Equity). Инвесторы получают пакет акций компании в обмен на обещанные деньги.

---

[47] Если целевая сумма не достигнута, инвесторы получают свои деньги обратно.

[48] Впервые одноранговое (P2P) кредитование было введено в Великобритании в 2005 году, тогда объем средств, предоставленных через пиринговые платформы, достиг 64 млрд долларов США. Ожидается, что к 2025 году объем торговли достигнет 1 трлн долларов [591].

Реализация концепции Crowdfunding в современной экономике осуществляется стремительными темпами. Так, в США с использованием механизмов Crowdfunding с 2012 по 2017 год объем финансирования увеличился с 2,7 млрд долларов до 95,9 млрд долларов в год. В странах Европы Crowdfunding рос со средним показателем в 146% в год [70]. Этот рост обусловлен резким ростом рынка Великобритании (на который приходится 73% всего европейского рынка) и быстрым расширением рынков альтернативного финансирования в небольших европейских странах Северной Европы, Пиренейского полуострова и стран Балтии. Вторым по величине европейским рынком является Франция, на долю которой приходится 22% европейского рынка Crowdfunding, затем следует немецкий рынок – 15,6% [176].

Китай – лидер рынка альтернативного финансирования, на долю которого приходится 99,2% всего рынка Crowdfunding в Азиатско-Тихоокеанском регионе. В 2017 году объем финансирования с использованием Crowdfunding составил 5,5 млрд долларов [176]. Согласно отчету Всемирного банка, к 2025 году данная отрасль в Китае достигнет размера 50 млрд долларов [589, 590]. При этом следует отметить, что в КНР модель P2P кредитования изначально построена на кредитных гарантиях[49], однако некоторые FinTech компании начали переходить к модели резервного фонда кредитного риска[50][564]. P2P модель кредитования в основном представляет собой гибридную модель, в которой платформы анализируют информацию о проекте или заявителе в оффлайн режиме, используя традиционные методы оценки кредитоспособности для оценки кредитных рисков. Заявки, которые соответствуют критериям, публикуются онлайн для финансирования инвесторами. При этом большинство крупных P2P-кредиторов имеют физические филиальные сети по всей стране. Модель онлайн-кредитования FinTech предполагает финансирование в основном за счет розничных инвесторов. Платформы сотрудничают с третьими сторонами для привлечения новых заемщиков. Важно отметить, что крупные китайские платформы вышли за рамки кредитования и превратились в продукты по управлению активами, страхованию бизнеса и

[49] Платформы генерируют кредит под высокие процентные ставки, предлагают инвесторам более низкую, но гарантированную норму прибыли, зарабатывая на спреде.

[50] Резервный фонд позволяет снизить кредитный риск для инвесторов, укрепить доверие инвесторов. Концептуально данный механизм аналогичен резервам под обесценение портфелей, которые традиционные банки обязаны хранить для своих кредитных портфелей в соответствии с нормативными требованиями.

предоставлению финансовых услуг, охватывающего все сегменты клиентов. В настоящее время в КНР доминируют три услуги: P2P-финансирование, проведение платежей с использованием мобильного телефона и Crowdfunding [592].

В Великобритании P2P платформы[51] позиционируют себя в качестве розничных инвесторов, как альтернативу банковским депозитам, а не как рискованный инвестиционный инструмент. Цель состоит в том, чтобы обеспечить низкий, стабильный доход для розничных инвесторов и предоставить кредиты по низким ставкам индивидуальным заемщикам и малым предприятиям [564].

По оценкам Goldman Sachs, в течение ближайших пяти лет 11 млрд долларов из 150 млрд годовой прибыли банков США могут быть потеряны из-за развития FinTech-кредитования посредством одноранговых платформ [564].

Важнейшим элементом концепции FinTech является алгоритмическая торговля (Algorithmic Trading, AT). Автоматизация инвестиций и другие новые технологии изменили структуру рынков капитала. Используя высокоскоростные и высокопроизводительные вычисления, сложные инструменты и алгоритмы, алгоритмические трейдеры (algorithmic traders[52]) получили возможность осуществлять торговлю ценными бумагами на основных фондовых биржах по всему миру [176]. В настоящее время акции и деривативы в основном торгуются в электронном виде – с использованием цифровых приложений, автоматизированных и роботизированных подходов к управлению, которые применяют ML/AI и самонастраивающиеся алгоритмы для выбора и выполнения торговых стратегий [559]. Высокочастотная торговля (High-Frequency Trading, HFT) – основная форма алгоритмической торговли на финансовых рынках, в которой современное оборудование и алгоритмы используются для быстрой торговли ценными бумагами. Анализ показывает отсутствие общего определения HFT, вместе с тем регулирующие органы выделяют две основные особенности HFT:

1) автоматизацию торгового процесса;

2) высокую скорость транзакций и отправки (отмены) заказов.

---

[51] Одними из крупнейших платформ P2P-кредитования являются Funding Circle, Zopa, Lend-Invest и RateSetter.

[52] Общая торговая активность может быть разделена на две основные категории: алгоритмическая торговля (AT) и неалгоритмическая торговая деятельность (non-algorithmic trading NAT), в зависимости от того, используют ли участники рынка алгоритмы для принятия торговых решений без вмешательства человека.

В отличие от развитых государств, в развивающихся странах цифровизация финансового сектора экономики осуществляется по направлению расширения использования мобильных финансовых услуг.

Мобильные финансовые услуги относятся ко всем финансовым транзакциям, проводимым через мобильное устройство. Поэтому он включает в себя мобильный банкинг, мобильные деньги и мобильные платежи. Другие услуги, предлагаемые в качестве мобильных финансовых услуг, включают услуги страхования и микрофинансирования [593].

Концепция Мобильного банкинга («Mobile Banking») включает в себя выполнение действий с традиционным банковским счетом, таких как получение информации об учетной записи и проведение операций по счетам. Мобильный банкинг предлагается крупными банками в развитых странах и обычно использует приложение для мобильных устройств, такое как приложение для смартфона, для безопасного выполнения банковских транзакций. Взаимозаменяемо с термином «Мобильный банкинг» используется термин «Мобильные деньги» («Mobile Money»)[53]. С технологической точки зрения

[53] История онлайн, электронного банкинга или интернет-банкинга началась в начале 1980-х годов [595]. В 1981 году четыре банка в Нью-Йорке (Citibank, Chase, Chemical и Manufacturers Hanover) решили предложить ограниченные электронные финансовые услуги по телефону с использованием системы видеотекста, «электронной технологии передачи и поиска информации, обеспечивающей интерактивную связь, в целях сбора и распространения данных, а также электронного банковского обслуживания и совершения покупок между, как правило, большими и разнообразными компьютерными базами данных и пользователями домашних или офисных терминалов, подключенных к телефонным, или кабельно-телевизионным линиям, или посредством использования сигналов телевизионного вещания». Это последовало в 1983 году, когда Банк Шотландии предложил членам Ноттингемского строительного общества услугу интернет-банкинга под названием «Home-link», использовавшую телевизор и телефон для проведения финансовых транзакций и оплаты счетов. Стэнфордский кредитный союз создал первый сайт для онлайн-банкинга, а в 1995 году Президентский сберегательный банк стал первым банком в Америке, предложившим счета через Интернет. Одна из причин, по которой эти попытки проникнуть в мир онлайн-банкинга стали возможными, заключалась в том, что Microsoft Money встроила онлайн-банкинг в свое персональное финансовое программное обеспечение в 1994 году. По мере продолжения 1990-х годов все больше банков и финансовых учреждений добавляли услуги онлайн-банкинга в свои предложения до тех пор, пока в 2005 году Федеральный экзаменационный совет по финансовым учреждениям объявил о новых правилах и положениях, касающихся онлайн-банкинга, уделив особое внимание рискам, безопасности и обучению клиентов. Почти каждое финансовое учреждение сегодня предлагает онлайн-банкинг через веб-браузеры. Выпуск Apple iPhone в 2007 году и других смартфонов в конце 2000-х годов спровоцировал переход от компьютерного банкинга к цифровому благодаря внедрению приложений для мобильного банкинга. В последние годы созданы банки, которые являются полностью интернет-банками. Например, Ally Bank (www.ally.com), ING Direct (www.ingdirect.com) и Банк Интернета США (www.bankofinternet.com/bofi).

мобильные деньги – это учетная запись, доступ к которой осуществляется с мобильного телефона пользователя[54]. Они могут быть использованы для оплаты товаров и услуг, могут быть отправлены от плательщика получателю. Ряд исследователей использовали термин «мобильные деньги» для обозначения возможности переводить деньги и (или) оплачивать товары и услуги, без необходимости иметь банковский счет [594]. Важно отметить, что мобильные деньги являются FinTech-институтом цифровой экономики, который представляет новую систему опосредованных цифровыми платформами отношений между банковскими (финансовыми) компаниями либо операторами связи, с одной стороны, и пользователями данным услуг – с другой.

Мобильные платежи – это оплата товаров и услуг посредством личного мобильного устройства в качестве терминала транзакций, предполагающие использование традиционного банковского счета или счета мобильных денег[55].

---

[54] Обычно он управляется оператором мобильной связи, отдельно от учетной записи телефона пользователя.

[55] Деньги поступают из двух основных источников, включая средства клиентов, расположенные в банках в форме депозитного счета или кредитного счета (в том числе карты предоплаты), или средства клиентов с сохраненной стоимостью, поддерживаемые операторами мобильных сетей (mobile network operators MNO). В некоторых юрисдикциях такие счета могут также принимать форму текущего счета, карточного счета, платежного счета или счета транзакции. Таким образом, мобильные платежи финансируются за счет ссылок на счета или платежные инструменты (кредитные карты не обязательно связаны с учетной записью) и отличаются с точки зрения рисков. Клиенты могут «заплатить заранее» (с помощью карты предоплаты, подарочной карты, предоплаты в MNO), «заплатить сейчас» (с помощью дебетовой карты или номера банковского счета) или «заплатить позже» (с помощью кредитной карты или телефона). Тем не менее основные модели мобильных платежных услуг на африканском континенте представляют собой средства клиентов с сохраненной стоимостью, поддерживаемые операторами мобильных сетей (модель MNO), а также сочетание банка, оператора мобильной связи или другой третьей стороны, предлагающей связь и услуги по финансовым транзакциям, которые сочетают в себе характеристики как чистого банка, так и модели чистого MNO (гибридной модели). Гибридная модель представляет собой комбинацию банка, оператора мобильной связи или иной третьей стороны, которая предлагает услуги связи и финансовых транзакций. Эта комбинированная гибридная модель называется моделью MNO/Bank. В соответствии с этой моделью платежные сервисы на основе мобильной телефонной компании, которые обрабатывают платежи внутри компании с помощью ввода/вывода денежных средств через агентскую сеть MNO, связаны с официальными банковскими услугами, такими как сбережения, кредиты и страхование, через партнерство с регулируемым финансовым учреждением, обеспечивая связь с банком и переводы между платежным счетом мобильного телефона пользователя и счетами в банке. Большинство мобильных финансовых услуг являются гибридными, опираясь на относительные преимущества участвующих партнеров. Таким образом, это позволяет тем, у кого нет официальных банковских счетов, иметь возможность совершать сделки с теми, у кого есть официальные банковские счета, и тем самым включать их в официальную финансовую систему.

Консалтинговая компания Innopay классифицирует мобильные платежные системы по двум критериям: удаленность и бизнес-модель. Платежи по показателю удаленности классифицируются на основе физического местонахождения потребителя (в непосредственной близости от прилавка магазина или удаленных платежей, таких как онлайн-платежи через мобильный телефон). Платежи по критерию бизнес-модели характеризуются уровнем взаимодействия с потребителями (Peer to Peer (P2P) или Consumer to Consumer (C2C)) или сотрудничеством между компаниями и клиентами (Business to Consumer (B2C) [596].

Специфика развития направления цифровизации мобильных платежей предполагает тесное сотрудничество телекоммуникационных компаний и банковских институтов [63]. Более того, цепочка создания стоимости мобильных платежей может включать операторов мобильной связи, поставщиков финансовых услуг[56], сторонних поставщиков платежных услуг[57], поставщиков услуг[58], поставщиков оборудования[59], системных интеграторов, продавцов и потребителей мобильных телефонов [597].

Исследователи выделяют в основном четыре типа операционных моделей мобильных платежей по критерию организации-драйвера данного финансового механизма [598, 599]:

1) под руководством оператора мобильной связи (MNO). В данной модели сборы за мобильные транзакции взимаются непосредственно MNO без участия банков[60]. Телекоммуникационные компании становятся квазибанками[61] [600];

---

[56] Например, банки, финансовые союзы и т. д.

[57] Например, Alipay, Google Wallet и Paypal.

[58] Например, компании общественного транспорта, школы, коммунальные предприятия.

[59] Например, производители микросхем, мобильных телефонов и поставщики терминального оборудования.

[60] При осуществлении мобильных платежей учетная запись мобильного телефона, подключенная к номеру телефона пользователя, обычно считается платежной учетной записью. Поэтому платежи за потребительские покупки товаров или услуг вычитаются непосредственно с мобильного счета. Таким образом, банки не участвуют и ничего не получают от транзакции.

[61] Такие фирмы, как PCCW, Smartone, PLDT и KT, разрабатывают финансовые приложения для своих услуг и получают сборы. IT-компании, такие как Google и Facebook, поглощают банковские услуги. Facebook, возможно, создает новые способы соединения маркетинга, финансирования, рекламы и лояльности клиентов, о которых не мечтали всего несколько лет назад. У Apple теперь есть Apple Pay. Такие кредитно-карточные компании, как Visa, Mastercard и American Express, в настоящее время выходят и захватывают традиционную банковскую деятельность, имея карты, которые связаны с банковскими счетами, и эксклюзивные соглашения с такими розничными сетями, как Walmart.

2) под руководством банка. Банки предлагают услуги мобильных платежей независимо, в то время как мобильные телефоны являются лишь одной из платформ оплаты. MNO несут ответственность только за предоставление канала доступа к информации, но не участвуют в эксплуатации и управлении платежными системами; поэтому банки несут полную ответственность за транзакции и сохраняют всю прибыль;

3) под руководством сторонней платформы. В данной модели сторонние платежные системы создают платформу поддержки торговли, которая заключает контракты отдельно с банками. Эти платежные системы имеют финансовую основу и надежную репутацию в отрасли, и они не зависят от других финансовых учреждений[62];

4) гибридные модели. MNO сотрудничают с одним или несколькими выбранными банковскими учреждениями для предоставления услуг мобильных платежей. MNO и банки стремятся работать вместе, чтобы доминировать на рынке, поскольку их сотрудничество может использовать преимущества присутствия первого в сети и взаимоотношений с клиентами, а также опыт последнего в области технологий электронных платежей, безопасности и управления кредитами, в то же время устраняя взаимные недостатки.

Следует выделить следующие факторы, стимулирующие рост мобильных платежей в развивающихся странах [601].

1. Социально-экономические условия. Большинство людей в странах с развивающейся экономикой не имеют текущего счета, кредитной и дебетовой карты. Плохо развитая инфраструктура в сочетании с высокими тарифами за услуги по переводу денег делают мобильные платежи привлекательными [602].

2. Экономическая эффективность. Большинство транзакций, проводимых в развивающихся странах, сочетают малый размер каждой отдельной операции, но большие совокупные объемы [603]. Вместе с тем создание платежной инфраструктуры, включая открытие

[62] На сторонних платежных платформах потребитель покупает товары у поставщиков, перечисленных платформой, и платформа информирует продавца о доставке. Платформа будет переводить деньги с банковского счета покупателя продавцу, но не будет делать этого до тех пор, пока покупатель не получит и не проверит товар и не одобрит оплату. Он соединяет потребителей, банки и продавцов, используя оператора мобильной связи в качестве платформы. Платежные платформы не только могут обслуживать потребителей независимо от того, с каким банком они ведут бизнес, что в противном случае сложно, но также могут защитить покупателей от продавцов-мошенников.

отделения банка, является коммерчески нерентабельным, поскольку требует значительных первоначальных инвестиций[63].

3. Распространение мобильных телефонов (ввиду снижения стоимости они становятся более доступными для населения развивающихся стран).

4. Удобство в использовании и осуществлении финансовых транзакций (появляется возможность осуществления платежей без привязки к конкретным платежным терминалам или отделениям банковских организаций).

5. Новые инициативы (существует несколько новых инициатив международных организаций и неправительственных организаций, таких как Международная финансовая корпорация, Всемирный банк, Фонд Гейтса, GSMA и другие, способствующие внедрению мобильных платежных систем).

Исследование, проведенное Беком, Памуком, Урасом, показало положительную корреляцию между использованием мобильных денег и торгового кредита [552, 604].

Вместе с тем следует отметить ряд факторов, которые ограничивают дальнейший рост мобильных платежей [593]:

1) жесткие правила и ограничения со стороны регуляторов;

2) монополистические устремления в коммерческой деятельности банков;

3) ограничения в развитии сотрудничества с традиционными банковскими институтами[64];

4) слаборазвитая экосистема, включая недостаточное обеспечение современной инфраструктурой, отсутствие стандартов, перегрузки в телекоммуникационной сети, отсутствие необходимой квалификации и навыков пользования [605];

---

[63] Включает оборудование, инфраструктуру, а также сотрудников отдела кадров и службы безопасности. Банковские операции вне филиала выглядят более привлекательными, поскольку они используют местные ресурсы и локальную инфраструктуру, а также оборудование и человеческие ресурсы, такие как мобильные телефоны и агентские магазины. Стоимость типичного перевода мобильного платежа составляет около 1%. Например, стоимость перевода денег через MTN и Wizzit в Южной Африке составляет всего около 0,05 доллара США.

[64] Например, M-PESA потребовалось более пяти лет для получения возможности сотрудничать с коммерческими банками, чтобы его клиенты могли снимать деньги в банкоматах банка. Сотрудничество важно, так как большинство традиционных банков обычно не имеют вспомогательных инструментов для работы с мобильными платежами.

5) проблемы безопасности. Население развивающихся стран чаще становится жертвой киберпреступников [606] поскольку, во-первых, развивающиеся страны не имеют эффективных современных правовых рамок и механизмов борьбы с киберпреступностью; во-вторых, пользователи уделяют меньше внимания вопросам безопасности; в-третьих, отсутствует цифровая грамотность. В большинстве случаев мобильные платежные системы не имеют отдельного набора правовых норм, особенно в развивающихся странах [607].

Важно отметить положительную динамику развития концепции «мобильных денег» в мировой экономике. Так, если в 2006 году в мире всего 10 организаций предлагали услуги мобильных денег [63, 608], то в 2014 году они получили распространение в 89 странах [609]. По итогам 2019 года количество организаций, предоставляющих мобильные платежные услуги, превысило 280, при этом взрывной рост поставщиков отмечен в 2010–2016 годах. При этом, по оценкам OMFIF, в ближайший год количество пользователей мобильных платежей достигнет 1,5 млрд человек [583].

Вместе с тем мобильные платежные системы демонстрируют большие различия в уровнях проникновения на разных национальных рынках. Они медленно распространяются в Европе, Соединенных Штатах и других странах, где кредитная система является зрелой и хорошо развитой, а система оплаты кредитными картами пользуется большой популярностью [597, 610, 611]. Имея доступ к сравнительно менее развитым системам потребительских банковских и кредитных карт, потребители в Японии и Южной Корее быстро акцептировали технологии мобильных платежей, в результате чего рынки мобильных платежей в этих странах стали более развитыми [612]. В 2020 году проникновение мобильных платежей в Китае достигло 86%: с внедрением оплаты по QR-кодам продавцы смогли снизить транзакционные издержки, не устанавливая платежные терминалы[65] [613]. Согласно данным Центрального банка Ганы [614], по состоянию на сентябрь 2018 года в Гане насчитывалось 12,5 млн активных пользователей мобильных платежей (около половины населения страны), что в пять раз больше, чем в 2014 году. Количество зарегистрированных счетов мобильных денег в Бангладеш в 2018 году увеличилось более чем вдвое по сравнению

[65] Комиссия за мобильные и онлайн-платежи в Китае составляет менее 0,6%.

с 2014 годом, и за тот же период число зарегистрированных агентов увеличилось на 51% [594]. Платежные сервисы, страховые и банковские стартапы аккумулируют значительные внешние инвестиции, лидером по привлечению которых по состоянию на 2021 год является компания Grab (Сингапур).

Безналичные транзакции в Великобритании через мобильные приложения, цифровые кошельки и платежи с помощью QR-кодов неуклонно росли и, по оценкам, в 2019 году превысили 1 трлн долларов [583]. Цифровые платежи развивались параллельно с электронной коммерцией и другими цифровыми услугами и достигли в 2019 году 3,5 трлн долларов, что почти втрое больше по сравнению с 1,3 млрд долларов в 2014 году.

Согласно данным OMFIF, по результатам 2020 года розничные онлайн-расходы в Китае достигли 2 трлн долларов. Объем мобильных транзакций, по данным Народного банка Китая, в 2018 году достиг 61 млрд долларов (по сравнению с 1,7 млрд в 2013 году). В настоящее время китайский рынок мобильных платежей оценивается 5,7 трлн долларов. Две доминирующие платформы мобильных платежей в стране – Alipay и WeChat Pay обеспечивают 93% этих транзакций[66][583].

При анализе цифровизации финансового сектора необходимо рассмотреть сектор страхования, в котором внедрение современных технологий, направленных на повышение эффективности, объединение рисков и управление претензиями, привело к формированию концепции InsurTech.

Как отмечено в ряде исследований [176], современные модели страхования стали более адаптивными, создающими условия для постоянно растущего потока данных через различные гетерогенные источники, такие как датчики или социальные сети. Внедрение технологий аналитики Big Data позволило предприятиям InsurTech использовать конкурентные преимущества перед другими участниками рынка. Важнейшим аспектом является аккумулирование цифровых данных, генерируемых окружающими устройствами, датчиками, которые позволяют более точно рассчитывать страховые риски.

[66] Одна из причин успеха мобильных кошельков в Азии заключается в том, что они произошли от популярных цифровых сервисов, по которым уже проводился большой объем транзакций. Alipay позволил осуществлять мобильные платежи для гиганта электронной коммерции Alibaba. WeChat Pay облегчил переводы между контактами в приложении для обмена сообщениями.

В данном контексте выделяют три основные области цифровизации, в которых генерируемые Big Data влияют на эффективность страхования [615].

1. Vehicle telematics (телематика транспортного средства) предполагает использование мобильных технологий для мониторинга и оценки поведения каждого отдельного водителя и формирует тем самым индивидуальную модель расчета страховых рисков[67] [616].

2. Wearables («умная одежда») позволяет аккумулировать биометрическую информацию, включая данные о физической активности, показателях жизнедеятельности и здоровья, что дает возможность повысить точность расчета рисков для компаний, работающих в сфере медицинского страхования и страхования жизни.

3. IoT позволяет генерировать и аккумулировать информацию из новых источников данных[68].

В разрезе формирования концепции InsurTech, отдельных бизнес-процессов страхования цифровизация затрагивает ключевые сегменты: аналитика данных и рисков, продажи, управление, расследование случаев мошенничества, управление активами.

В данном контексте выделяют три основные тенденции цифровизации страхования [615]: персонализация, расширение клиентской базы и упрощение процедур. Цифровые технологии позволяют страховщикам получать информацию об изменении поведения потребителей и предлагать персонализированное покрытие рисков. Благодаря возможностям Big Data и AI, формируются новые модели микрострахования, особенно в развивающихся экономиках. Отмечается, что цифровизация страховой деятельности может снизить неоперационные издержки компаний на 30–50%, сократить компенсационные расходы на 1–3% и увеличить собираемые премии на 1–3%. Цифровизация операционных процессов, оптимизация IT-платформы и внедрение более эффективных вычислительных систем позволяют компаниям значительно улучшить коммерческие и организационные характеристики [559]. Согласно отчету Morgan Stanley о страховании и технологиях, внедрение цифровых

---

[67] Устройства с телематической технологией (также известные как «черный ящик») могут определять различные показатели вождения, такие как местоположение, время суток, пробег, частота движения, поведение в опасных зонах, скорость, скорость ускорения и привычки торможения. Затем эти метрики могут быть рассмотрены в более точной и индивидуальной модели ценообразования.

[68] Например, позволяют страховщику потенциально двигаться в направлении упреждающего управления рисками.

технологий дает возможность страховым компаниям иметь доходность на 10% выше, чем в среднем на рынке, и быть на 20–30% более прибыльными [617].

Одним из самых перспективных направлений формирования цифровой экономики является разработка и реализация концепции Central Bank's Digital Currency, CBDC (цифровая валюта центрального банка). Издержки центральных банков, связанные с эмиссией и распространением бумажных денег, высоки и постоянно растут[69]. Сокращение этих затрат является одним из ключевых преимуществ реализации концепции CBDC.

Согласно определению Официального форума валютно-финансовых институтов (OMFIF), цифровая валюта центрального банка – это деньги центрального банка в цифровой форме, которые служат новым средством платежа и альтернативой наличным деньгам [581]. CBDC выражена в официальной денежной единице страны-эмитента и является прямым обязательством центрального банка.

Важно отметить, что концепция CBDC находится в стадии активного изучения как на уровне теории, так и практики реализации. В настоящее время, как показал проведенный анализ, в экономической литературе по критерию доступности выделяют две формы цифровых валют центрального банка:

1) розничные (Retail CBDC), предполагающие всеобщий доступ к обязательствам центрального банка, фактически представляют собой цифровую версию фиатной валюты центрального банка;

2) оптовые (Wholesale CBDC), предполагающие доступ, ограниченный коммерческими банками и расчетными палатами, формирующие межбанковский рынок [618].

Отсутствие единой технологии внедрения и циркуляции CBDC позволяет выделить два основных механизма по критерию централизации: прямой и гибридный.

При прямом (централизованном) механизме центральные банки осуществляют выпуск, распределение и управление CBDC без какого-либо вмешательства со стороны коммерческих финансовых учреждений.

При гибридном (децентрализованном) механизме центральные банки высвобождаются от необходимости взаимодействия с большим количеством розничных клиентов и выполнения задач, которые

[69] Оценки для зоны евро и Канады показывают, что общая стоимость распределения и обслуживания денежных средств составляет около 5% ВВП [581].

дублируют операции коммерческих банков. Гибридный механизм предполагает, что финансовые посредники несут ответственность за осуществление платежей в режиме реального времени и выполняют задачи, связанные с управлением клиентскими активами и обеспечением безопасности, следуя стандартам «Знай своего клиента» (KYC) и ПОД-ФТ (противодействия отмыванию денег и финансированию терроризма) в рамках рекомендаций FATF.

Основные характеристики CBDC, согласно отчету Банка международных расчетов, подготовленного в 2020 году совместно с Европейским центральным банком, Федеральной резервной системой США, Банком Англии, Банком Японии, Банком Канады, Риксбанком (ЦБ Швеции), Национальным банком Швейцарии [619], должны включать инструментальные, системные и институциональные составляющие.

А. Инструментальные требования:

1) конвертируемость – возможность обмена CBDC по номинальной стоимости на наличные и частные деньги;

2) удобство – платежи с использованием CBDC должны быть простыми, как использование наличных денежных средств, платежных карт или платежных функций цифровых устройств, для стимулирования их принятия и расширения доступности;

3) признание и наличие – использование для тех же типов транзакций, что и наличные средства, в том числе в торговых точках и между физическими лицами, включая возможность совершать офлайн-транзакции (возможно, в течение ограниченного периода времени до заранее определенных пороговых значений);

4) низкие тарифы – платежи с использованием CBDC должны осуществлять по низким тарифам или бесплатно для конечных пользователей.

Б. Системные требования:

1) безопасность – инфраструктура и участники системы CBDC должны быть устойчивы к кибератакам и другим угрозам, включая эффективную защиту от подделок;

2) скорость расчетов – мгновенный (или почти мгновенный) окончательный расчет должен быть доступен конечным пользователям системы;

3) устойчивость – система CBDC должна быть устойчивой к операционным сбоям, стихийным бедствиям, отключениям электричества и другим рискам. У конечных пользователей должна быть

возможность совершать офлайн-платежи, если сетевые подключения недоступны;

4) доступность – конечные пользователи системы должны иметь возможность совершать платежи 24/7/365;

5) пропускная способность – система должна быть способна обрабатывать очень большое количество транзакций;

6) масштабируемость – система CBDC должна иметь возможность расширяться с учетом будущих объемов транзакций;

7) совместимость – система должна предлагать достаточные механизмы взаимодействия с цифровыми платежными системами и механизмами частного сектора, чтобы обеспечить легкий переток средств между системами;

8) гибкость и адаптивность – система CBDC должна быть гибкой и адаптируемой к меняющимся условиям и политическим императивам.

B. Институциональные требования:

1) надежная правовая база – центральный банк должен иметь четкие полномочия, необходимые для выпуска CBDC;

2) стандарты – система CBDC (инфраструктура и участвующие организации) должна соответствовать нормативным стандартам[70].

Вместе с тем, как показывает анализ, использование CBDC приведет к существенному изменению платежной инфраструктуры как на внутреннем, так и на международном уровнях.

В данном контексте, с учетом традиционного функционала банковских регуляторов, к новым целям центральных банков целесообразно отнести следующие:

а) максимизация эффективности CBDC в выполнении функций валюты, а именно как средства обмена;

б) обеспечение безопасности CBDC как средства сохранения стоимости;

в) обеспечение стабильности CBDC как единицы учета экономических и финансовых операций [620].

Для реализации представленных целей экспертами выделены, в том числе, следующие задачи, стоящие перед центральными

[70] Например, организации, предлагающие передачу, хранение или хранение CBDC, должны соответствовать эквивалентным нормативным и пруденциальным стандартам, как компании, предлагающие аналогичные услуги за наличные или существующие цифровые деньги.

банками, для эффективного использования технологического потенциала CBDC.

1) обеспечение финансовой и макроэкономической стабильности;

2) содействие экономическому росту и благосостоянию;

3) реализация актуальной и эффективной денежно-кредитной политики;

4) улучшение финансовой доступности (инклюзивности) для населения;

5) повышение безопасности, надежности и устойчивости банковской системы;

6) борьба с финансированием терроризма и отмыванием денег [581].

Анализ показывает, что комплексность и сложность задачи внедрения концепции CBDC компенсируются целым рядом преимуществ, которые она предоставляет финансовому рынку, в том числе:

а) повышение эффективности банковской деятельности за счет снижения затрат на транзакции;

б) увеличение доходов центрального банка от сеньоража;

в) усиление мониторинга транзакций для целей налогообложения и выявления преступной деятельности;

г) улучшение характеристик трансграничных платежей [619].

Исследование, осуществленное Банком Англии в 2016 году [621], показало, что эмитированная CBDC в объеме, равном 30% ВВП, стимулирует прирост объема производства почти на 3% благодаря снижению реальных процентных ставок и затрат на денежные операции. CBDC является дополнительным инструментом денежно-кредитной политики, который может существенно улучшить способность центрального банка стабилизировать деловой цикл.

Более того, эксперты указывают на потенциал новых возможностей для центральных банков с введением CBDC с точки зрения политики обеспечения ценовой и финансовой стабильности, информационной безопасности [622].

Проведенный анализ показал превалирующий характер в современной экономической литературе при оценке влияния CBDC на политику государственного регулирования экономики монетарных моделей, основными субъектами которых выступают домашние хозяйства (через размещение депозитов, которые коммерческие

банки преобразуют в кредитные денежные средства; CBDC, созданные центральными банками и эмитированные через обмен на государственные облигации), коммерческие банки (создающие новые кредитные деньги за счет новых депозитов), органы государственного управления (посредством реализации фискальной политики, монетарной политики с учетом нового цифрового инструментария CBDC). Например, как показали исследования, представленные Барди и Камхофом [623], с точки зрения монетарной политики центрального банка использование технологии CBDC позволяет значительно сократить ограничения ликвидности коммерческих банков, вызванные условиями привлечения и проведения банковских операций с депозитами, которые связаны с транзакционными издержками и выступают своего рода «квази-налогами на ликвидность» для заемщиков, негативно влияющими на условия кредитования реального сектора экономики[71].

Важным условием эффективного внедрения CBDC с точки зрения монетарной политики является их реализация коммерческим банкам в обмен на краткосрочные государственные облигации. При этом волатильность спроса на новый инструмент в условиях финансовой стабильности можно регулировать двумя методами:

1) эмиссией ограниченного объема CBDC в условиях свободного рыночного определения процентной ставки по ним (количественное правило);

2) эмиссией, определяемой совокупностью эндогенных факторов, в условиях свободного рыночного определения объема CBDC (ценовое правило).

Данный инструментарий позволяет использовать CBDC в качестве механизма контрцикличного регулирования экономики (сокращение объема CBDC в условиях экономического бума, и наоборот, увеличение объема в кризисных условиях), стабилизируя, таким образом, экономический цикл и снижая инфляцию [624].

Аналогичным образом Бордо и Левин [625] отмечают, что процентная ставка CBDC может служить основным инструментом денежно-кредитной политики. Уполномоченные органы государственного регулирования получают инструментарий для снижения

[71] Важно учитывать, что в современной экономике именно коммерческие банки генерируют более 95% денежной массы.

рыночных процентных ставок ниже нуля в ответ на внешние или внутриэкономические шоки. Центральный банк сможет обеспечить соответствующую степень денежно-кредитной адаптации, не прибегая к количественным смягчениям. Операционные процедуры центрального банка будут более прозрачными, направленными на покупку (продажу) краткосрочных государственных ценных бумаг, обеспечивающими баланс спроса и предложения на CBDC.

В качестве преимущества инструментария CBDC Центральный европейский банк (ECB) [626] выделяет использование механизмов отрицательных процентных ставок, «вертолетных денег» и прочих дополнительных монетарных механизмов. При этом если замена наличных денежных средств на CBDC представляется малорискованной, поскольку осуществляется простая замена одной формы денег центрального банка на другую без изменения остальной финансовой системы, то замена на CBDC банковских депозитов увеличивает зависимость банков от кредита центрального банка и в целом уменьшает депозиты до востребования в банковской системе.

С точки зрения фискальной политики, как отмечают Барди и Камхоф [624], внедрение CBDC будет способствовать увеличению, при прочих равных условиях, фискальных доходов в текущих консолидированных (правительство плюс центральный банк) потоках (consolidated fiscal income flows) за счет снижения чистых процентных расходов (net interest expenses). Это позволит фискальному органу увеличить расходы или снизить налоговые ставки при неизменных целевых показателях дефицита и долга[72].

На фоне активного обсуждения роли регуляторов в обеспечении стабильности финансовых систем в связи с расширением использования частных криптовалют центральные банки изучают практические возможности перехода на CBDC.

---

[72] Следует отметить, что цифровизация затрагивает и другие важные элементы финансовой инфраструктуры государств. В 2020 году в России введена в эксплуатацию цифровая платформа Федеральной налоговой системы (ФНС) для взаимодействия с банками, построенная на технологии распределенного реестра (Блокчейн) [627]. В качестве перспективных ФНС выделяет такие направления цифровизации, как применение Блокчейн-платформы для новых госпрограмм поддержки бизнеса, безбумажное предоставление услуг клиентам банков в рамках расчетно-кассового обслуживания и кредитования, а также «формирование досье клиента и профилирование его рисков». На 2021 год было запланировано создание цифровой платформы для передачи административных данных в другие заинтересованные госорганы.

Так, согласно отчету Банка международных расчетов (BIS), около 20% центральных банков стремятся запустить цифровую валюту в ближайшие 6 лет [584]. В 2020 году 84 центральных банка изучали возможность имплементации концепта CBDC в денежно-финансовые системы своих стран [628]. По прогнозам Европейского аналитического центра, к 2030 году по меньшей мере три государства заменят свою фиатную валюту на CBDC [629]; в отчете немецкого аналитического центра по финансовым технологиям прогнозируется, что от трех до пяти стран полностью заменят свою валюту цифровой валютой центрального банка [630]. Комитету по платежам и рыночной инфраструктуре, Центру инноваций Банка международных расчетов, МВФ и Всемирному банку главами G20 в октябре 2021 год поручено было провести анализ потенциальной роли CBDC в расширении трансграничных платежей и последствий их использования для международной валютной системы [631].

Составным элементом цифровизации современных банковских систем является внедрение цифровых расчетных систем центральных банков, концепции RTGS (Real-Time Gross Settlement)[73]. Проблематика использования устаревших технологических решений[74] определяется отсутствием поддержки для проведения расчетов в режиме 24/7, подверженностью техническим сбоям и сложностям при проверке и расчетах по определенным сделкам. Оценки показывают, что страны тратят от 0,5% до 0,9% своего валового внутреннего продукта на транзакционные издержки розничных платежей [583]. Помимо высоких затрат, платежные системы отстают от технологических инноваций или перехода к цифровой экономике. Вместе с тем развитие технологий мгновенных платежей создало предпосылки для внедрения механизмов передачи платежных сообщений и обеспечения доступности исходных средств для получателя в реальном времени почти круглосуточно. Данное внедрение современной цифровой инфраструктуры

[73] Транзакции между счетами в разных коммерческих банках проводятся через центральный банк – систему расчетов в реальном времени (RTGS), которая обеспечивает перемещение средств в реальном времени между счетами коммерческих банков в центральном банке.

[74] Великобритания использует автоматизированную платежную систему клиринговой палаты (известную как Chaps), США – Fedwire, а в зоне евро – Target-2.

поставит операционную банковскую деятельность на новую основу, полностью или частично заменив SWIFT[75].

Кроме систем мгновенных межбанковских платежей, активно реализуются проекты мгновенных розничных платежей. В ходе исследования, проведенного в 2020 году компанией InfoSys, в мировой экономке выявлены 54 платежные системы, осуществляющие транзакции в режиме реального времени[76][583].

В 2020 году 16 крупнейших европейских банков из Испании, Франции, ФРГ, Нидерландов и Бельгии заявили о создании собственной системы мгновенных переводов [632]. В рамках инициативы финансовые организации планируют разработать технические решения для организации P2P-платежей между владельцами пластиковых карт (European Payments Initiative, EPI). Целью проекта является укрепление европейского рынка через стандартизацию технологий[77]. Вместе с тем существующая инфраструктура быстрых платежей, управляемая коммерческими банками, требует дополнительных катализаторов для инноваций и расширения использования.

---

[75] SWIFT – Общество всемирных межбанковских финансовых каналов связи, представляет собой сеть для безопасных трансграничных финансовых транзакций или денежных переводов, созданная в 1973 году в Бельгии. Она доминирует на мировом рынке денежных переводов. По сути система SWIFT является системой обмена сообщениями. Система SWIFT может доставлять только сообщения о транзакциях. Платеж обрабатывается через обычную банковскую систему. Поэтому процесс транзакции SWIFT можно разделить на две части: доставку сообщений и расчет платежей. Проблема SWIFT заключается в ликвидности и кредитном риске, поскольку бизнес-модель этой системы в значительной степени опирается на уровни банков, позволяющие совершать транзакции. Клиринговый центр или расчетный центр необходимы на стороне отправителя и получателя. Это делает весь процесс длительным [634]. В 2015 году SWIFT запустила Глобальную инициативу по платежным инновациям (Global Payment Innovation Initiative GPII) для улучшения традиционной системы обмена сообщениями. Это свод новых правил и соглашений об уровне обслуживания, которые банки и учреждения в сети SWIFT должны подписать. Он направлен на то, чтобы, предоставив функции клиенту, получать выгоду от платежей с использованием средств в тот же день, с возможностью низкой комиссии и прозрачности процесса, сквозного отслеживания платежей и передачи полной информации о платежах по денежным переводам.

[76] Современные банковские клиринговые и расчетные системы, созданные для обеспечения своевременной и эффективной обработки розничных платежей, включают Новую платежную платформу в Австралии, Службу Faster Payments в Великобритании, Swish в Швеции и FAST в Сингапуре.

[77] При помощи EPI, пользователи смогут осуществлять платежи в офлайн- и онлайн-магазинах и снимать наличные. Разработки станут дополнением к уже задействованным техническим решениям, которые работают в рамках международных платежных схем.

Коммерческие банки модернизируют действующую платежную инфраструктуру либо в сотрудничестве с центральными банками, либо под их давлением [583]. Формирование инфраструктуры систем быстрых платежей требует адаптации услуг между коммерческими и центральными банками[78].

Кроме того, банки вводят в оборот оказываемых услуг новые цифровые платформы. Аналитики Morgan Stanley отмечают, что в условиях цифровизации современные банки вынуждены изменять бизнес-модели по одному из двух направлений.

1. «Банковское дело – как услуга, Banking-as-a-Service» предполагает включение банковских услуг в предложения третьих организаций, что позволяет расширить источники доходов, но сопряжено с рисками растущей зависимости от этих посредников.

2. «Банковское дело – как платформа, Banking-as-a-Platform» позволяет банкам строить отношения с клиентами, предлагая собственные торговые площадки наряду с инструментами управления личными финансами[79] [633]. Исследование Райффайзенбанка и аналитического агентства B2B International в 2021 году [635] показало, что около 50% крупных российских компаний[80] включили следующие цифровые финансовые сервисы в основные критерии, определяющие их выбор коммерческого банка: цифровые продукты и сервисы, быстрый онлайн-доступ к финансированию и интеграция с ERP-системами. Сбербанк России заявил о намерении вывести на рынок новую Блокчейн-платформу[81], которая будет предоставлять

[78] Одним из основных изменений, необходимых для внедрения венгерской системы мгновенных платежей AFR, которая была запущена в марте 2020 года, стало создание новых механизмов для круглосуточного предоставления ликвидности коммерческими банками.

[79] В России, например, банки разрабатывают «суперприложения», с помощью которых клиенты могут получить доступ к банковским счетам для электронной коммерции, доставки еды, вызова транспорта и планирования поездок, а также других видов деятельности. Один банк поставил цель вывести нефинансовый бизнес с менее 1% операционного дохода (до резервов) примерно до 30% к 2030 году.

[80] 200 российских компаний с объемом годовой выручки от 538 млн рублей.

[81] Главной целью платформы является ускорение расчетов между контрагентами. Производительность новой платежной системы очень высока, что позволяет без перегрузок обрабатывать операции большого количества клиентов. Любая компания-клиент Сбербанка сможет получить доступ к смарт-контрактам, развернутым специалистами госбанка. У пользователей появится возможность запускать собственные смарт-контракты (Сбербанк отчитался о создании блокчейн-платформы для автоматических расчетов. – Режим доступа: https://whattonews.ru/sberbank-otchitalsja-o-sozdanii-blokchejn-platformy-dlja-avtomaticheskih-raschetov/. – Дата доступа: 31.07.2020).

услуги по покупке цифровых финансовых активов[82] [636]. Также рассматривается возможность выпуска собственной цифровой валюты – Сберкоин[83]. Сбербанк совместно с компанией S7 внедряет систему продажи авиабилетов для корпоративных клиентов с использованием Блокчейн-платформы, смарт-контрактов и – впервые в России – виртуальных токенов [637]. Это позволит отказаться от системы банковских гарантий и авансов, а также ускорит расчеты. В феврале 2020 года в регулятивной «песочнице» Центрального банка России успешно завершен пилотный проект Блокчейн-платформы для выпуска и оборота цифровых прав[84]. В Индии ряд ведущих банков[85] входит в число консорциумов из 11 крупных кредиторов, созданных для запуска первого в стране финансирования, связанного с Блокчейн, для МСП [284]. Новое отраслевое решение на основе Блокчейна обеспечит ряд преимуществ, в том числе: сокращение сроков финансирования цепочки поставок, снижение затрат, углубление зоны охвата кредитов и увеличение количества МСП, интегрированных в кредитную систему [638]. В 2021 году Bank of New York Mellon (BNY Mellon) заявил о намерении проведения операций с Bitcoin и другими криптовалютами, для которых банк разработал прототип платформы, позволяющей осуществлять транзакции с криптовалютами так же, как это происходит с традиционными активами [639].

---

[82] Банк России выразил намерение усилить регулирование банков, желающих развивать собственные экосистемы и платформы нефинансовых услуг. Дано определение экосистемы – это совокупность сервисов, в том числе платформенных решений, позволяющих в рамках единого процесса получать широкий спектр продуктов и услуг. Такая конструкция по ЦБ несет серьезные риски для клиентов банков, экономики и государства в целом. На горизонте трех-пяти лет к таким участникам рынка будут повышаться требования к капиталу и раскрытию отчетности. Ключевой риск, который видит ЦБ в «неконтролируемом» развитии экосистем при участии банков, рост так называемых иммобилизованных активов на балансе. В отличие от кредитов это вложения, по которым не возникают требования к возврату денежных средств (ЦБ ограничит для банков строительство экосистем. – Режим доступа: https://www.rbc.ru/finances/23/06/2021/60d2db9c9a79471e3d878324?from=from_main_5. – Дата доступа: 23.06.2021).

[83] С января 2021 года в России вступил в силу закон «О цифровых финансовых активах», который введет их в правовое поле, предоставив возможность проведения экспериментов в этом направлении.

[84] Она позволяет оцифровывать (токенизировать) товары, услуги, ценные бумаги и другие активы. Особенность площадки – возможность выпуска гибридных токенов, обеспеченных одновременно различными активами.

[85] В том числе Standard Chartered, Mumbai ICICI, HDFC, Kotak Mahindra и Axis.

Важной составляющей формирования цифровой инфраструктуры банков является ее укрепление на низовом уровне. Быстрое распространение таких технологий, как смартфоны, AI, Big Data, появление новых конкурентов – FinTech-компаний, и изменения в отношении и поведении клиентов являются стимулом для банков к преобразованию и инновациям.

Современное развитие цифровой инфраструктуры коммерческих банков направлено, главным образом, на цифровизацию предоставляемых клиентам услуг, предотвращение мошенничества, автоматизацию филиалов, совершенствование цифрового банкинга и увеличение расходов на аналитические инструменты[86][640]. Ряд исследований показал, что около 80% банков инициировали проекты, имеющие отношение к технологии Блокчейн [260, 641]. При этом отмечается значительное повышение эффективности при внедрении технологий Блокчейн для выстраивания банковской инфраструктуры. Так, согласно расчетам Santander Innoventures, Блокчейн позволит традиционным банкам сократить расходы на инфраструктуру на сумму не менее 20 млрд долларов в год[87] [642, 643]. По мнению компании Accenture, технологии Блокчейн предоставят возможность инвестиционным банкам сократить расходы на инфраструктуру на сумму не менее 12 млрд долларов в год [644] и до 10 млрд долларов для поддержки клиринга [645]. В сфере оптового банкинга компанией CLS Group, ведущим поставщиком расчетных услуг на валютном рынке, для осуществления платежей запущен Блокчейн Hyperledger [646]. Крупнейший банк Сингапура DBS в 2021 году начинает операции по обмену криптовалюты с использованием Биткойнов, Эфира, Ripple [647]. В 2019 году французский банк Societe Generale

[86] ВТБ в 2020 году построил фабрику роботов, которые заменят сотрудников, в частности, в сфере кредитования. В 2021 году банк планирует «расширить штат» 60 цифровыми специалистами, к концу 2022 года – 250. ВТБ рассчитывает, что новые роботы позволят сократить долю рутинных операций по обработке документов и вводу данных, снизить стоимость процессов в 3–4 раза и ускорить их. В ВТБ робот уже обрабатывал заявки на льготные кредиты для малого и среднего бизнеса в рамках господдержки в период пандемии. Робот проверял до 1500 заявок в день и ускорил обработку в пять раз (ВТБ запустил фабрику роботов. – Режим доступа: https://www.vtb.ru/o-banke/press-centr/novosti-i-press-relizy/2020/07/2020-07-17-vtb-zapustil-fabriku-robotov/. – Дата доступа: 17.07.2020).

[87] Компании JPMorgan и Chase инвестируют средства в такие стартапы, как Axoni (Axoni Website. https://axoni.com), с целью снижения затрат на инфраструктуру (Goldman, JPMorgan to Invest in Blockchain Startup Axoni. – Режим доступа: https://www.reuters.com/article/us-axoni-blockchain-idUSKBN149073. – Дата доступа: 20.12.2016).

выпустил покрытую облигацию на сумму 100 млн. евро в качестве токена безопасности на публичной платформе Ethereum [648]. Банк JP Morgan использует Блокчейн для улучшения денежных переводов, банк HSBC – для службы безопасного хранения цифровых активов [649].

Кроме того, банковские институты активно начинают внедрять криптовалютные финансовые инструменты, построенные на технологии Блокчейн[88]. Ряд банков начали принимать криптовалюту на депозит[89]. Осуществляется взаимодействие между платежными системами и банками по предоставлению услуг по покупке криптоактивов[90].

Перспективным направлением цифровизации банковской инфраструктуры является использование Cloud Computing [91]. В настоящее

[88] В декабре 2020 года объявлено о подготовке немецким банком Bankhaus von der Heydt (BVDH) (основанным в 1754 году) первого прямого выпуска стейблкоина на Stellar. Проект осуществляется совместно с поставщиком технологии токенизации и хранения цифровых активов Bitbond (One of the World's Oldest Banks Is Issuing a Euro Stablecoin on Stellar. – Режим доступа: https://www.coindesk.com/one-of-the-worlds-oldest-banks-is-issuing-a-euro-stablecoin-on-stellar. – Дата доступа: 9.12.2020).

[89] Депозиты клиентов, использующих цифровую валюту, в настоящее время составляют почти 16% от общего объема депозитов в Signature Bank в Нью-Йорке. В ходе телефонного разговора Signature сообщила, что депозиты клиентов в криптоиндустрии теперь составляют 10 млрд долларов – вдвое больше, чем у калифорнийского конкурента Silvergate Bank (Signature Bank Crosses $10B in Deposits From Crypto Customers. – Режим доступа: https://www.coindesk.com/signature-bank-crosses-10b-in-deposits-from-crypto-customers. – Дата доступа: 22.01.2021).

[90] Компания Visa анонсировала выпуск собственной системы (API) для покупки криптовалют, которая будет интегрирована банками. Запуск продукта запланирован на конец текущего года. Первым пользователем сервиса станет цифровой банк First Boulevard (Visa поможет банкам предоставлять услуги по покупке и продаже биткоина. – Режим доступа: https://www.rbc.ru/crypto/news/601ab2ee9a7947a977dbffa7. – Дата доступа: 03.02.2021).

[91] Societe Generale Societe Generale (SocGen) со штаб-квартирой во Франции и его дочерние компании используют публичное облако, включая SaaS. В 2013 году люксембургский частный банк Societe Generale Bank & Trust завершил двухлетний проект по переводу своей основной банковской системы в частное облако. В марте 2017 года SocGen объявил, что с июня 2017 года будет использовать внешние общедоступные облачные сервисы от Microsoft и AWS для некоторого не клиентского контента, такого как финансовые исследования и маркетинговые данные. К 2021 году SocGen планирует иметь 80% своей инфраструктуры во внутренних и внешних облачных сетях. В 2015 году Deutsche Bank заключил сделку с Hewlett Packard Enterprise на оптовую банковскую инфраструктуру – «выделенные услуги центров обработки данных по требованию, включая системы хранения, платформы и хостинг» – эффективно управляемое частное облако, включая специализированную версию гибридного облака Helion OpenStack с открытым исходным кодом.

время банки рассматривают облако как «движущий фактор роста», а не просто как средство снижения издержек[92], позволяя упростить операционную деятельность, внедрить новые финансовые продукты и повысить гибкость [650, 651]. Другим фактором является то, что клиенты отдают предпочтение взаимодействию с банками через разные интерфейсы, включая онлайн и мобильный.

Рост агрегируемых банками Big Data[93], совершенствование технологий их обработки, анализа, инструментария управления информационной базой открывает новый спектр услуг для финансового сектора и большой потенциал для специализации и индивидуализации его продуктов [359, 651].

ML и AI стали ключевым фактором в сфере банковских услуг. Согласно ряду исследований [652], наибольшую эффективность данные технологии нашли в таких банковских операционных задачах, как оценка кредитоспособности клиентов[94], расчет эффективности работы филиалов, внедрение цифрового банкинга, проведение сегментации клиентов и реализация стратегии их удержания, прогнозирование рисков банкротства и мошенничества [653, 654, 655].

Исследователи выделяют также цифровизацию банковской операционной деятельности по управлению рисками, как одного из самых дорогостоящих и трудоемких процессов[95] [176]. Концепция реализации системных решений по внедрению цифровых технологий AI / ML для выполнения задач по повышению эффективности оценки кредитных рисков и предоставлению отчетности в рамках требований регуляторов получила название RegTech[96].

---

[92] В зависимости от области операционной деятельности банков, где использовались облачные технологии, сокращение затрат достигает 50%, в некоторых случаях банку HSBC удалось сократить до 90% затрат.

[93] Цифровые устройства генерируют огромные массивы цифровых данных, которые требуют анализа для обнаружения скрытых шаблонов.

[94] Кредитный скоринг позволяет банкам решать, следует ли предоставлять кредит физическому лицу.

[95] Например, BBVA, второй по величине банк в Испании, имеет 8000 из 137 000 сотрудников, работающих в департаменте compliance.

[96] RegTech был впервые определен как отдельное, развивающееся направление в финансовой индустрии, в Бюджетном отчете Казначейства Великобритании за 2015 год, а затем всесторонне исследован в Правительственной организации науки Великобритании (Government Office for Science) [176]. Согласно определению Управления по финансовому регулированию и надзору Великобритании (Financial Conduct Authority FCA), «RegTech – это подмножество FinTech, фокусирующееся на технологиях, которые могут облегчить выполнение нормативных требований более эффективно и действенно» [563].

Линн, Иуни, Розати, Кумминс определяют RegTech как информационную технологию[97], которая:

а) позволяет компаниям управлять нормативными требованиями и императивами соответствия путем определения воздействия нормативных положений на бизнес-модели, продукты и услуги, функциональную деятельность, политику, операционные процедуры и средства контроля;

б) обеспечивает соответствие бизнес-систем и данных;

в) дает возможность контролировать и управлять нормативными, финансовыми и нефинансовыми рисками[98];

г) позволяет формировать отчетность в соответствии с нормативными требованиями.

Современная финансовая система в рамках регуляторных требований по противодействию отмыванию денег и финансированию терроризма (ПОД-ФТ) Группы разработки финансовых мер борьбы с отмыванием денег (FATF) переходит от подхода, основанного на принципах «Знай своего клиента» (KYC), к подходу «Знай свои данные» (KYD) [563]. Таким образом, распространяется новая нормативная парадигма, затрагивающая широкие аспекты цифровизации, – от цифровой идентификации до суверенитета данных. В 2018 году пять крупнейших банков Северной Европы объединились с целью формирования совместной инфраструктуры по борьбе с отмыванием денег – Nordic KYC Utility. Инфраструктура на основе AI призвана содействовать в соблюдении правил и требований KYC. HSBC внедрил технологию AI, разработанную компанией Quantexa, для мониторинга внутренних бизнес-процессов и ПОД-ФТ. Royal Bank of Scotland и Vocalink в Великобритании разрабатывают систему ML для сканирования транзакций клиентов МСП

[97] Ключевым в этой области является IBM после приобретенной ими компании Promontory (стартап RegTech), и теперь они предлагают ряд решений на основе AI для сокращения расходов RegTech [176].

[98] Исследования, опубликованные The Trade, показывают, что только в 2016 году банки потратили более 100 млрд долларов на соблюдение нормативных требований, и эта стоимость растет. По оценкам Bain & Co., расходы на риск управления и соблюдения нормативных требований (governance risk and compliance GRC) составляют 15–20% «расходов банка» и 40% «расходов банка» соответственно. Если рассматривать конкретные правила, то закон Dodd Frank (США) обошелся в 36 млрд долларов, а MiFID II (ЕС) – в 2,5 млрд евро. Таким образом, с учетом существующей тенденции предполагается, что в ближайший год стоимость соблюдения нормативных требований возрастет с 4 до 10% от доходов финансовых учреждений [176].

с целью выявления фальшивых счетов и потенциальных случаев мошенничества [176].

Таким образом, к тенденциям цифровизации финансовой инфраструктуры следует отнести не только усиление конкуренции FinTech и банков, но и расширение взаимодействия между данными институтами. Специализированные отраслевые решения [129] разрабатываются банками в сотрудничестве с FinTech, при этом данное взаимодействие предоставляет банкам преимущество первопроходца в формировании и масштабировании новых бизнес-моделей.

Согласно исследованию российской Ассоциации ФинТех и компании Accenture [656], в 2023 году основные приоритеты банков в сфере цифровизации будут заключаться в следующем:

1) безопасный финансовый рынок: противодействие киберугрозам и мошенничеству. Отмечено отсутствие формализованного обмена информацией по финансовым мошенничествам между участниками рынка, а также отсутствие требований к информационной безопасности технологических компаний, которые предоставляют финансовые услуги (FinTech, Telecom, E-Commerce), и неоднозначность регулирования в этой области;

2) среда для развития финтех-инноваций: выстраивание целостной финтех-экосистемы. Отмечена сложность перехода стартапов к этапу пилотирования продукта из-за высоких издержек на интеграцию в процессы банка. Проблемой является небольшое количество участников в сегменте финтех-стартапов и ограниченное предложение финтех-решений для крупных игроков;

3) развитие механизмов доступа к данным, включая сведения из государственных систем, открытых и частных источников, в том числе авторизованные клиентами личные данные. Нет достаточного количества решений и технологических стандартов для обмена данными;

4) развитие платежной среды: удобных, прозрачных и понятных, быстрых и безопасных цифровых платежных услуг на основе эффективной и надежной платежной инфраструктуры;

5) невидимые финансы: новые возможности для легкого и бесшовного встраивания различных финансовых продуктов и услуг в бизнес игроков любых отраслей, то есть модель «финансовые услуги как сервис». Развитию этой отрасли могут помешать, прежде всего, ограничения для бесшовного встраивания электронной цифровой подписи в голосовые сервисы, мобильные приложения, мобильные устройства для предоставления финансовых продуктов

и услуг, а также отсутствие регулирования и инфраструктуры для взаимодействия через открытые API;

6) развитие конкуренции и регулирование экосистем.

Дальнейшая цифровизация платежных и расчетных платформ, как показывают исследования OMFIF, позволит сделать следующий шаг в направлении разработки национальной платформы «цифровой идентификации» (биометрическая технология электронного KYC), предназначенной для повышения безопасности и предотвращения возможного мошенничества. Кроме того, цифровая идентификация позволит сделать более эффективным доступ к услугам и авторизации платежей, повысить безопасность цифровых платежей [583]. Обновленная или новая платежная инфраструктура должна соответствовать целям политики финансовой доступности и стабильности, а также обеспечивать безопасность, функциональную совместимость, надежность, устойчивость, скорость и максимальную эффективность. Банк России объявил о планах создания единой платформы для оценки риска проведения сомнительных операций в банковской системе в 2018 году. Концепция платформы под названием ЗСК («Знай своего клиента» – аналог KYC) предполагает проведение скоринга банковских клиентов по критериям риска[99] [657].

Банки стремятся улучшить идентификацию новых клиентов, надежно аутентифицировать существующих клиентов и защищать ценные транзакции. Компания Goode Intelligence [658] прогнозировала, что к 2020 году биометрические показатели будут использовать 1,9 млрд клиентов банков по всему миру, что принесет доход в 4,8 млрд долларов компаниям, занимающимся внедрением биометрических систем в банковскую индустрию.

Тенденции, способствующие внедрению биометрических методов в банках:

1) рост мобильной и мультимодальной цифровой биометрической аутентификации;

2) появление биометрических банковских карт. Благодаря встроенным датчикам отпечатков пальцев они считаются жизнеспособным и удобным способом укрепления безопасности без ущерба для качества обслуживания клиентов;

[99] Оценка позволит относить банковских клиентов к трем зонам по принципу светофора (красной, желтой и зеленой). Кредитные организации должны будут учитывать оценку регулятора при работе с компаниями.

3) создание биометрических платформ. Банки начинают развертывать единую биометрическую платформу для поддержки нескольких банковских каналов и обеспечения идентификации, аутентификации и борьбы с мошенничеством[100];

4) использование биометрических технологий для проверки подлинности личности в Интернете при цифровой регистрации клиентов, открывающих новые банковские счета;

5) интеграция алгоритмических решений по выявлению мошенничества, противодействию мошенническим схемам, аутентификации на основе рисков, включая принятие поведенческой биометрии / аналитики;

6) различная скорость внедрения технологий в разных регионах в зависимости от наличия зрелых национальных систем идентификации, которые поддерживают биометрические данные. Банки будут использовать биометрические показатели для управления этой инфраструктурой, что приведет к созданию биометрических данных в качестве услуги, управляемой совместно частным сектором и государством. Регуляторы уже инициировали внедрение биометрии как части двухфакторной и многофакторной аутентификации[101];

7) внедрение технологий распознавания лиц (Facial recognition technology), AI/ML;

8) расширение применения биометрии для доступа к банкоматам в регионах, где эта технология уже была внедрена (Япония, Восточная Европа и Южная Америка), и ее развертывание в других регионах, где ПИН по-прежнему является основным механизмом аутентификации.

Важным элементом цифровизации финансовой инфраструктуры являются биржи. Одним из наиболее активно внедряемых биржевыми платформами технологических решений, предполагающих цифровизацию основной деятельности, является Блокчейн. Среди преимуществ данного вида торговли выделяют: ускорение проведения операций, снижение рисков, более низкие издержки на администрирование операций и тарифы на их проведение, P2P торговля, более надежный процесс проведения сделок [204].

---

[100] Одна платформа поддерживает несколько биометрических модальностей, которые могут быть сопоставлены с соответствующим каналом, – голосовая связь для контакт-центров и IoT, мультимодальная биометрия для мобильных устройств и Интернета и проверка отпечатков пальцев или сосудов для банкоматов.

[101] К ним относятся PSD2 ЕС, руководящие принципы FFIEC США и законодательство Банка Китая и Кореи.

Ряд исследователей [659] предложил рассматривать в качестве цифровых платформ также управление активами, поскольку управляющие организации выступают связующими звеньями между эмитентами ценных бумаг и инвесторами. Исследователи определили данные цифровые площадки на рынке ценных бумаг как Digital asset management platforms (DAMP) («Платформы цифрового управления активами»), призванные обеспечить значительную экономию затрат для инвесторов, радикально разрушая существующие бизнес-модели.

Выделяют четыре основных типа DAMP.

1. Индексные (пассивные) фонды (index (passive) funds) являются самыми старыми из существующих DAMP, представляют собой простые алгоритмические фонды. Преимуществом данной формы DAMP является минимум комиссионных платежей со стороны инвесторов, который достигается благодаря возможности эффективно использовать информационный арбитраж[102].

2. Биржевые фонды (Exchange Traded Funds, ETF) представляют собой подмножество индексных фондов, которые дают возможность дополнительно улучшить функциональную эффективность путем реструктуризации процесса управления фондами в формат двусторонней рыночной платформы. ETF трансформируют рынки ценных бумаг, позволяя переупаковывать рыночные индексы и продавать их как ценные бумаги на этих рынках[103].

3. Платформы поддержки управляющих активами (asset manager support platforms) обеспечивают взаимодействие между

---

[102] Индексные фонды являются очень простыми алгоритмическими фондами, которые позволяют инвесторам пассивно покупать и держать пересечение всего рынка, таким образом устраняя обычный механизм управления фондами аналитиков, трейдеров и т. д. Вместо того чтобы гоняться за валовой прибылью любой ценой, индексные фонды конкурируют за цену, максимизируя чистую прибыль, снижая операционные накладные расходы до минимально возможного уровня и в то же время зарабатывая валовую прибыль. Индексные фонды существенно трансформируют управление активами, прежде всего радикально снижая отраслевые сборы и занятость.

[103] ETFs не управляются как обычные фонды, а скорее структурированы как двусторонние рыночные платформы. С одной стороны, инвесторы покупают и продают акции ETF на вторичном рынке; с другой стороны, арбитражеры (например, инвестиционные банки) обменивают определенные корзины ценных бумаг с ETF на «единицы создания», то есть эмиссии и обратные покупки акций ETF на первичном рынке, так что поддерживается выравнивание: 1) между рыночной стоимостью портфеля ETF и рыночной стоимостью его акций; 2) структурой портфеля ETF и индексом, который он отслеживает. Эта архитектура платформы позволяет ETF достичь исключительно низких эксплуатационных расходов.

управляющими фондами и рынком ценных бумаг. Они предоставляют услуги как активным, так и пассивным менеджерам, включая управление рисками портфеля, оптимизацию и исполнение торговых операций, а также поддержку соответствия нормативным требованиям. В отличие от простоты индексных фондов, они используют сложную управляемую данными аналитику, чтобы повысить как фундаментальную эффективность оценки, так и функциональную эффективность рынка ценных бумаг. Наиболее значимой платформой являются Aladdin от BlackRock[104], под управлением которой в 2017 году находились активы стоимостью около 20 трлн долларов США [660].

4. Роботизированные советники (robo-advisors) являются новейшими DAMP, которые на практике в основном выступают в роли дистрибьюторов ETF. Данные платформы предназначены для розничного рынка продуктов управления фондами. На базовом уровне робо-советники служат онлайн-инструментами сравнения цен, предлагая клиентам инвестиционные продукты с наилучшими условиями [661][105]. Сектор охватывает управление активами стоимостью около 140 млрд долларов США (на конец 2017 года), его рост составляет 50–100% в год [662]. К преимуществам данных DAMP можно отнести следующее [615]:

а) прозрачная структура комиссионных и низкие затраты;

б) предотвращение конфликта интересов – банки обычно рекомендуют продукты для инвестирования «не выходя из дома»;

в) круглосуточный контроль портфеля, без выходных, оптимизация (ребалансировка) портфеля и продажа ценных бумаг с убытком для компенсации налогового обязательства по приросту капитала;

---

[104] Он был разработан в конце 1980-х годов как внутренний инструмент управления рисками для портфелей облигаций и впоследствии превратился во всеобъемлющую «операционную систему», которая продается управляющим активами в виде облачной подписки, «платформа Aladdin сочетает в себе сложную аналитику рисков с комплексными инструментами управления портфелем, торговлей и операциями на единой платформе для обеспечения принятия обоснованных решений, эффективного управления рисками, эффективной торговли и оперативного масштаба» BlackRock (2018). Кроме того, Aladdin предлагает инструменты, которые в целом повышают «функциональную эффективность» управления активами в таких областях, как оптимизация и исполнение торговых операций (в обход инвестиционных банков), до подготовки нормативных документов. По мере роста масштабов, масштабов и сложности Aladdin, он все больше стирает границы между человеческим и алгоритмическим управлением.

[105] Робо-советники также обычно разрабатывают индивидуальные портфели продуктов на основе ситуации и предпочтений клиента.

г) автоматизация развития и процесса поиска новых моделей, адаптированных для работы на конкретных рынках;

д) использование управляющими данных активов в качестве инструментов для улучшения инвестиционного процесса.

К недостаткам относят следующее.

1) избыточно сложный или плохо разработанный алгоритм находит ложные корреляции из данных;

2) хрупкость в реальных кризисных рыночных ситуациях;

3) недостаточно тщательный сбор информации об инвесторах;

4) отсутствие творческих подходов, особенно в условиях кризиса.

Важно отметить, что большая доля отрасли управления активами находится под управлением трех компаний – BlackRock, Vanguard и State Street [663, 664], которые контролируют свыше половины рынка индексных фондов, действуя не только как горизонтальные монополии (олигополии) в отдельных сегментах DAMP, но и вертикальные, усиливающие контроль над всеми сегментами рынка[106].

По мнению Скардови, с развитием стабильных, безопасных и быстрых взаимосвязанных цифровых платформ будет снижаться роль дилеров-брокеров в корпоративных облигациях, так как универсальные торговые площадки могут кардинально изменить динамику рынка облигаций и в пользу непосредственных участников (покупателей и продавцов)[107][559]. Цифровые платформы фактически позиционируют себя в качестве потенциального конкурента фондовых бирж. Их конкурентное преимущество основывается на цифровой (информационной) составляющей, а также дополнительной ценности прикладной аналитики. Цифровые платформы функционируют в качестве торговых площадок, без необходимости обязательного привлечения банковских структур и регулируемых фондовых рынков.

Следующим FinTech элементом являются криптобиржи. Данные цифровые торговые площадки предоставляются участникам биржевой торговли, могут обменять криптовалюту на фиатные деньги или другие криптовалюты с использованием цифровых кошельков,

---

[106] Увеличивающийся масштаб позволяет крупнейшим провайдерам еще больше сократить расходы (сборы), что, в свою очередь, привлекает дополнительных клиентов.

[107] 60% европейских государственных облигаций сейчас торгуются в электронном виде, а также 25% мирового объема торгов корпоративных облигаций инвестиционного класса и 13% для высокодоходных корпоративных облигаций.

которые создаются биржами для каждого пользователя в своей системе [665]. Биржи обладают закрытыми ключами кошельков пользователей, хранят личную и банковскую информацию клиента.

Современная концепция криптовалюты представлена в 2009 году в исследовании С. Накомото [666], в рамках которого были обозначены основные подходы к построению новой крипто-финансовой системы[108][667]. Данное направление получило высокую динамику развития в 2010 году благодаря конвергенции ряда технологий, среди которых ключевую роль играет Блокчейн. Технологии Блокчейн позволяют проводить мгновенные транзакции и формировать финансовые отношения без привязки к границам [254]. Исследования выявили ряд преимуществ использования данной технологии в финансовом секторе, среди которых, в технологическом разрезе, гарантия списания средств с одного счета и зачисления на другой счет без риска распределения одних и тех же средств более одного раза. В макроэкономическом разрезе внедрение технологий Блокчейн позволит сократить совокупные операционные банковские расходы на 20 млрд долларов, а стоимость денежных переводов – на 35%. При этом, по данным исследования [292], глобальные инвестиции в Блокчейн в банковском и финансовом секторах составили уже около 3 млрд долларов.

Проведенный анализ показал необходимость диверсификации цифровой валюты и криптовалюты. Так, цифровая валюта – это валюта, которую, можно конвертировать в фиатную валюту. Транзакции, осуществляемые через интернет-банкинг и мобильные приложения, платежи по банкам или по кредитным картам, являются в основном транзакциями в цифровой валюте, которые контролируются центральными банками стран и другими признанными государственными учреждениями. Они используются в рамках действующей нормативно-правовой системы. В современной экономике около 90% фиатных валют являются де-факто цифровыми валютами [667].

Криптовалюта – это форма цифровой валюты (например, Биткойн, Эфир). При этом общее определение криптовалюты на сегодняшний день отсутствует. Отметим некоторые подходы в определении криптовалюты. Так, ЕСВ отталкивается от цифровой и социальной природы криптовалют, определяет криптовалюты как

[108] Статья была опубликована человеком или людьми под именем Сатоши Накамото.

«тип нерегулируемых цифровых денег, которые выпускаются и обычно контролируются их разработчиками, используются и принимаются членами определенного виртуального сообщества»[109] [581]. Казначейство США исходит из валютно-финансовой роли криптовалют, определяя их как «средство обмена, которое функционирует как валюта в некоторых средах, но не обладает всеми атрибутами реальной валюты»[110]. Особенностью криптовалюты является отсутствие учреждения, определяющего ее стоимость: она создается с помощью сложных алгоритмов программирования[111], и ее стоимость определяется агрегированным предположением участников крипторынка, что является одной из причин ее нестабильности[112][595]. Таким образом, криптовалюта может быть определена как имеющий экономическую ценность цифровой объект, который создается (и регулируется) в соответствии с частным соглашением между сообществом или

---

[109] Virtual currency schemes / European Central Bank. October, 2012. 55 p. – Режим доступа: https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf?941883c8460133b7758f498192a3ed9e. – Дата доступа: 24.12.2021.

[110] Guidance / Application of FinCEN Regulations to Persons Administering, Exchanging, or Using Virtual Currencies. Financial Crimes Enforcement Agency. FIN-2013-G001. March 18, 2013. – Режим доступа: https://web.archive.org/web/20130319213642/http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html. – Дата доступа: 11.10.2021.

[111] Протокол определяет предложение криптовалюты, а также набор правил, обязательных для выполнения всеми участниками. Например, он утверждает, что может существовать не более 21 млн Биткойнов [668, 669].

[112] Вместе с тем, по мнению ряда исследователей, с коммерческой точки зрения первой криптовалютой является система eCash компании DigiCash, Inc., созданная в 1990 году. Платежи переводились онлайн и офлайн с использованием криптографических протоколов для предотвращения двойных расходов. Криптогрские протоколы также использовали слепые подписи для защиты конфиденциальности своих пользователей. Как первая криптовалюта, система eCash была доступна через различные банки и смарт-карты в разных странах, таких как США и Финляндия. eCash была централизованной системой, принадлежавшей DigiCash, Inc. и более поздним технологиям eCash. Однако после того, как InfoSpace была приобретена в 1999 году, eCash и криптовалюта отошли на второй план. e-Gold был пионером интернет-платежей. В качестве первой успешной системы онлайн-микроплатежей она стала пионером многих новых методов и методов электронной коммерции, которые впоследствии стали широко использоваться в других аспектах онлайн. Эти методы включают в себя оплату через зашифрованное соединение Secure Sockets Layer и предлагают интерфейс прикладного программирования, позволяющий другим веб-сайтам создавать сервисы с использованием транзакционной системы e-gold. Однако система не выполняла требования KYC и требования к отчетности о подозрительных транзакциях. С введением в действие Закона о патриотизме США соблюдение требований стало основной проблемой для денежных переводов. Кроме того, он должен бороться с хакерами и интернет-мошенничеством. До того, как в 2008 году было принято решение об изъятии и ликвидации всего золотого запаса e-gold в соответствии с законом о конфискации активов, e-gold обрабатывало операций с драгоценными металлами на сумму более 2 млрд долларов США в год.

пользователями и другими участниками сети. Криптосообщество управляет криптовалютами без прямого участия государства [670].

Общим подходом к определению криптовалют являются констатация их цифровой криптографической природы и отсутствие универсальности сферы ее применения. Представляется, что на текущем этапе становления данной концепции криптовалюта может быть охарактеризована как актив, имеющий цифровую криптографическую форму и используемый для нишевых операций в рамках отдельных экосистем (включая платежные), а также как спекулятивный инструмент на крайне волатильном рынке криптоактивов. В будущем развитие данной концепции, на наш взгляд, будет, главным образом, реализовываться в формате государственных цифровых валют (CBDC) и платежных инструментов онлайн платформ под нарастающим контролем со стороны специализированных органов государственного регулирования.

Поскольку криптовалюта в настоящее время не эмитируется центральным органом, она теоретически нечувствительна к вмешательству или манипулированию со стороны государства, и ценность криптовалюты зависит от того, сколько инвесторы готовы платить за нее в определенный момент [671].

Экосистема криптовалют, как правило, включает такие институты, как майнеры, пользователи, криптобиржи, поставщики услуг транзакций и разработчики программного обеспечения, а также поставщики рыночной информации и видеокарт, продавцы, принимающие криптовалюты в обмен на реальные товары и услуги (рис. 1.7).

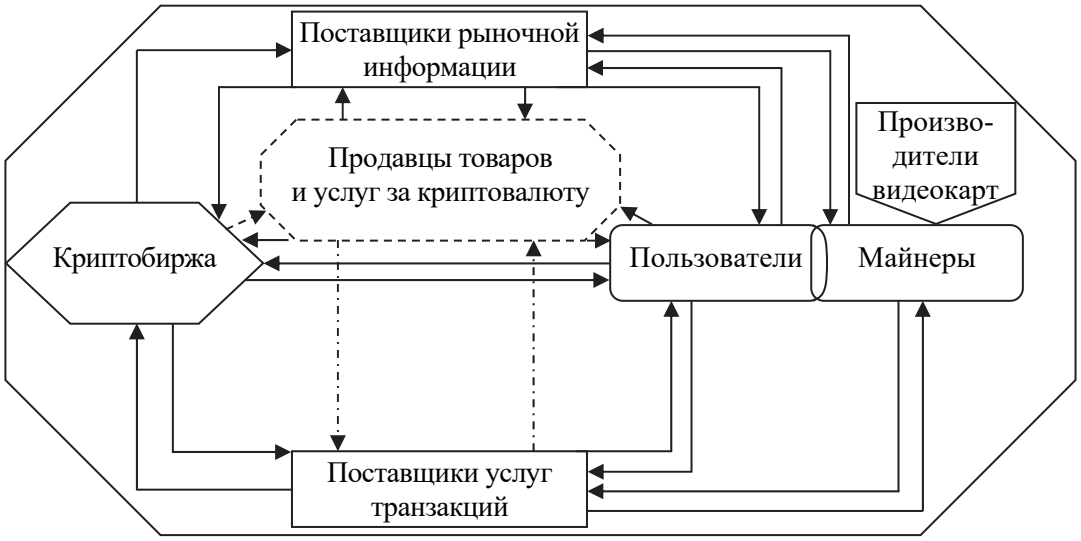


Рис. 1.7. Экосистема криптовалют (разработано автором на основе [670])

Майнинг криптовалют является стартовой операцией в системе циркуляции криптовалют и представляет собой сложную, заранее определенную вычислительную задачу, которая требует решения – математического доказательства работы [672]. Майнеры – это физические или юридические лица, которые используют специализированное программное обеспечение для генерации решений сложных алгоритмов (сложность решения увеличивается со временем) и проверки транзакций в криптовалютной сети[113] [670]. Блокчейн-сети вознаграждают майнеров Блокчейн за потребленные ими ресурсы[114]. Каждые 4 года происходит двукратное уменьшение выплачиваемого майнерам вознаграждения за майнинг Биткойнов[115] [673].

Экономическая эффективность майнига побуждает к формированию майнинговых пулов, призванных объединить вычислительные мощности и распределить вознаграждение в зависимости от вложенных ресурсов [674]. Исследование Рена и Уарда показало, что доля блоков, добытых в июле 2018 г. пулами, составляла 91,12% для Биткойна и 92,2% для Эфира. Несколько пулов для майнинга, такие как F2Pool и AntPool, контролируют большинство вычислительных ресурсов в сети цепочки блоков Биткойна [675, 676]. Согласно данным btc.com, около 55% совокупной вычислительной мощности (по состоянию на 05.02.2021) приходится на 4 крупнейших майнинговых пула: F2Pool, Poolin, BTC.com, AntPool.

Полученные в результате майнинга криптовалюты используются держателями криптовалют для реализации на бирже за фиатную валюту, приобретения отдельных товаров и услуг, осуществления прочих транзакций.

В некоторых исследованиях изучалась взаимосвязь между криптовалютами и различными обменными курсами или финансовыми

---

[113] Объем генерируемых Биткойнов ограничен 21 млн блоков.

[114] Таким образом, стоимость производства одного биткойна может быть определена количественно как затраты на его добычу. Есть два основных вида затрат: затраты на покупку оборудования и затраты на электроэнергию. С точки зрения стандартной экономики первое можно рассматривать как фиксированную стоимость, а второе – как предельные издержки [677].

[115] Так, за первые 210 000 блоков вознаграждение, выплачиваемое участникам с каждым проверенным блоком, составляло 50 Биткойнов. Начиная с 28 ноября 2012 года вознаграждение было уменьшено вдвое (халвинг) до 25 Биткойнов, а 9 июля 2016 года, после того как было добыто еще 210 000 блоков, вознаграждение было уменьшено вдвое до 12,5 Биткойнов за блок. 11 мая 2020 года произошло очередное снижение вознаграждения до 6,25 Биткойнов за блок. Майниг, как планируется, прекратится около 2140 г. [678].

активами[116]. Эмпирические результаты всех этих исследований подтверждают, что курсы Биткойна и других криптовалют не коррелируют с основными активами, такими как золото, нефть, облигации и индексы акций. Тем не менее, несмотря на обширные исследования криптовалют, взаимосвязи на рынке криптовалют изучены недостаточно.

По мнению Ермака, криптовалюты имеют признаки в большей степени присущие финансовым активами, нежели валютам, включая [679, 680]:

а) волатильность;

б) уязвимость к спекулятивным пузырям;

в) устойчивость к макроэкономическим шокам;

г) экстремальность значений в рыночном поведении.

В доказательство данного утверждения Совбетов, изучая факторы, которые влияют на цены пяти криптовалют (Биткойна, Эфира, Dash, Litecoin и Monero) как в краткосрочном, так и в долгосрочном периоде в 2010–2018 годах, используя метод ARDL[117] на еженедельной основе[118], выявил следующую корреляцию: повышение цен на золото, цены на нефть и индекса S & P 500 повышает цены на криптовалюты, в то время как повышение процентной ставки по облигациям США и индекса доллара США приводит к их падению [668, 671]. Это неблагоприятное влияние индекса доллара США и процентной ставки по облигациям США на цены криптовалют указывает на то, что при уменьшении доходности доллара США и облигаций США инвесторы предпочитают вкладывать средства в криптовалюты[119]. Результаты данного исследования показывают, что криптовалюты ведут себя больше как инвестиционный инструмент, чем как валюта, и цены на эти финансовые активы взаимодействуют со значительными макрофинансовыми показателями.

---

[116] Примеры включают исследования Yermack, Bouri, Baur, Lee, Corbet [680, 682, 683, 684, 685].

[117] Модели авторегрессионного распределенного запаздывания (ADL, autoregressive distributed lags) – модели временного ряда, в которых текущие значения ряда зависят как от прошлых значений этого ряда, так и от текущих и прошлых значений других временных рядов.

[118] В частности, исследуется взаимодействие между этими пятью криптовалютами и фондовым рынком (индекс SP500), ценами на золото и макроэкономическими показателями (процентная ставка).

[119] С другой стороны, криптовалюты, как и инвестиционные инструменты, движутся с аналогичной тенденцией индекса фондового рынка, цены на золото и нефти, которые являются общими рыночными индикаторами.

Таким образом, среди факторов, влияющих на стоимость криптовалют, выделяют макроэкономические, политические и законодательные, рыночные, формирующие спрос и предложение криптовалют. Кроме того, как показал ряд исследований, стоимость криптовалют определяется тройственностью таких факторов, как [681]:

1) национальное и международное регулирование рынка криптовалют[120];

2) киберпреступность в криптовалютной сфере, которая подрывает доверие к криптовалюте, а также порождает растущую необходимость в улучшении международной нормативно-правовой базы;

3) формирование финансовых пузырей[121], которые приносят вознаграждение участникам финансовых махинаций.

В экономической литературе отмечены различные подходы к классификации криптовалют. Так, Хайлмен классифицирует валюты на две категории: материальные и цифровые [672, 686]. Материальные валюты, тесно связанные с «товарными деньгами», получают свою ценность из относительного дефицита и нефинансовой полезности:

а) валюты с внутренней полезностью (currencies with intrinsic utility). Этот класс валюты включает телефонные карты с предоплатой и, в некоторой степени, смарт-карты с денежной стоимостью. Этот класс не зависит от управления, как в случае с денежными

---

[120] В январе 2018 года широко сообщалось, что финансовые регуляторы в Южной Корее стремятся сотрудничать с властями Китая и Японии по новым правилам торговли криптовалютой. В сообщении Yonhap News от 8 января говорится, что представители Корейской комиссии по финансовым услугам (FSC), а также представители соответствующих агентств Японии и Китая встретились в декабре 2017 года, чтобы обсудить надзор за инвестициями в криптовалюту. После последовавшего за этим выпуска новостей цены на криптовалюту упали, и Биткойн понес потери, превышающие 50% за один месяц.

[121] Несмотря на то, что цены на Биткойны значительно снизились, связанные со слухами о введении нормативных требований, даже с повсеместным запретом криптовалют в некоторых юрисдикциях, ослабление такого нормативного давления теоретически должно привести к значительному повышению цен. Кроме того, рост числа серьезных случаев киберпреступности продолжает подрывать доверие и стабильность на рынке криптовалют со значительными последствиями. Тем не менее наличие врожденных пузырей ценообразования приносит существенное вознаграждение тем, кто хочет получить прибыль от такой незаконной тактики, как взлом криптовалютного рынка во время кражи. Рост киберпреступности также порождает немедленную потребность в улучшении согласованности международного регулирования, но он также связан с повсеместным запретом таких финансовых инструментов в некоторых юрисдикциях, что приводит к дальнейшему расхождению в подходе к международному регулированию [681].

инструментами, и, что более важно, его внутренняя ценность не является абстракцией и не обязательно географически связана;

б) токены. Современными примерами являются местная валюта или валюта сообществ[122]. Данный класс валют имеет меньшую внутреннюю ценность, так как его использование более конкретно и обычно ограничивается некоторыми социальными контрактами или соглашениями, такими как предоставление их для обмена на товары или для ограничения поставок товаров;

в) централизованная цифровая валюта (centralized digital currency). Примерами являются баллы лояльности от финансовых, телекоммуникационных или розничных компаний; воздушные мили от авиакомпаний[123]. Структура управления централизована;

г) распределенная и (или) децентрализованная цифровая валюта (distributed and/or decentralized digital currency). Данная категория включает в себя криптовалюты, которые могут передаваться любым сторонним агентам, и их управление в основном децентрализовано. Нет юридического лица, ответственного за деятельность, и, следовательно, они выходят за рамки традиционного регулирования.

Криптовалюты также классифицируют по признаку универсальности использования [176].

1. Нативные валюты – это цифровые взаимозаменяемые активы, созданные внутри Блокчейн или «раздвоенные» из существующего Блокчейн. Они представляют собой класс активов электронных денег, универсально доступных через одноранговые платежные сети. При этом нативная валюта требует Блокчейн (в то же время Блокчейн может функционировать без нативной валюты). Новизна нативных валют по отношению к более традиционным формам денег заключается в том, что они объединяются с сетевой инфраструктурой, которая обеспечивает взаимный обмен валютами без посредников.

2. Криптотокены представляют собой формы «цифровых ваучеров», которые позволяют владельцам токенов получать доступ практически к любому виду услуг и активов: от денежных

[122] Такие как брикстонский фунт и бристольский фунт, которые используются в Англии, доллар Солт-Спринг в Канаде.

[123] Местные валюты, такие как Brixton Pound, BerkShares и Salt Spring Dollar, также подпадают под эту категорию, несмотря на то, что классифицируются как токены.

вознаграждений или товаров до пунктов лояльности и даже других криптовалют[124].

Общепринятая многими регуляторами классификация выделяет три основных класса токенов[125][176, 687]:

а) платежные токены (Payment tokens) – синонимичны криптовалютам в качестве средства оплаты за приобретение товаров и услуг или в качестве средства перевода денег или стоимости;

б) служебные токены (Utility tokens), предназначенные для обеспечения цифрового доступа к приложениям и (или) сервисам, построенным на основе инфраструктур на основе Блокчейн;

в) токены активов (долгов) (Asset / Debt tokens), выполняющие функцию акции (доли), для инвестора они представляют такие активы, как долговые обязательств, собственные ценные бумаги;

г) гибридные токены, характеризующиеся комбинацией трех предыдущих признаков.

Среди преимуществ использования криптовалютных активов в финансовом секторе выделяют следующие [670, 688, 689, 690]:

1) криптовалюты позволяют значительно сократить расходы на перевод средств через международные границы;

2) возможность прямой одноранговой транзакции устраняет или существенно сокращает операционные издержки и временную задержку;

3) упрощение и повышение экономической эффективности микроплатежей;

4) развитие краудфандинга для малых и средних предприятий;

5) усиление безопасности платежей;

6) использование в качестве альтернативы валютам благодаря имеющимся свойствам хеджирования, ликвидности и диверсификации.

Более того, криптовалютная технология формирует платформу для более эффективных мобильных или цифровых транзакций в будущем.

---

[124] Разработка новых токенов, как правило, является менее сложным процессом, чем создание валют, поскольку для этого не требуется изменять коды из определенного протокола или формировать новый Блокчейн с нуля. Кроме того, недавняя реализация промежуточного программного обеспечения и инструментов разработки Блокчейн, полных кодов Тьюринга для интеллектуальных контрактов в цепочке блоков, позволяет легко создавать, публиковать, распространять и обмениваться криптокенами.

[125] Включая Швейцарский орган по надзору за финансовым рынком (FINMA 2018).

Отсутствие жесткого регулирования и относительно простой механизм создания токенов формируют условия для новой тенденции финансирования компаний, особенно стартапов. Вместо привлечения средств по традиционным каналам (выпуск акций или получение займа) стартап-проекты и компании с целью привлечения внешнего финансирования получают возможность осуществлять продажу собственной криптовалюты за фиатные деньги или другие активы посредством таких FinTech механизмов, как первичное размещение монет (ICO) и первичное размещение акций (первоначальное биржевое предложение (initial exchange offerings IEO)[126] [673]. За последние несколько лет ICO стали инновационным механизмом финансирования, позволяющим привлекать корпоративных инвесторов[127] [691].

Как правило, ICO-проект выпускает токен в публичном Блокчейн и продает токен потенциальным инвесторам для сбора средств на ранних стадиях разработки без привлечения посредников и в обход строго регламентированного и регулируемого процесса привлечения капитала, свойственного венчурным инвесторам или банкам [692]. Фактически, ICO – это нерегулируемые выпуски токенов, которые представляют некоторые права в сообществе Блокчейн (обычно права на использование и гораздо реже права на работу или права на активы) [586, 693]. В данном контексте токены – это единицы стоимости, предназначенные для обеспечения полезности или для работы в качестве ценных бумаг, которые предоставляют владельцам права на результаты проекта «по мере их поступления»[128][694, 695]. Как правило, данные токены являются криптовалютами, которые предназначены для обращения в собственной экосистеме предприятия и, в отличие от традиционных, долевых и долговых ценных бумаг, не имеют конкретных и осуществимых юридических прав [696].

---

[126] В отличие от ICO, механизм IEO опирается на криптовалютные биржи, чтобы гарантировать надежность потенциальных проектов и связать высококачественные проекты с потенциальными инвесторами [692].

[127] Первая ICO была проведена в июле 2013 года Mastercoin, цифровой валютой, построенной на Блокчейн Биткойна (Here's The Man Who Created ICOs And This Is The New Token He's Backing. – Режим доступа: https://www.forbes.com/sites/laurashin/2017/09/21/heres-the-man-who-created-icos-and-this-is-the-new-token-hes-backing/?sh=336cbeec1183. – Дата доступа: 21.09.2021).

[128] Стартап-проекты также могут использовать эирдроппинг, то есть бесплатную рассылку токенов инвесторам для ознакомления с их проектами.

Процесс первичного предложения монет (ICO) состоит из трех отличительных этапов [176]:

1) первоначальный отчет или предложение (white paper announcement), в котором компания представляет потенциальным инвесторам бизнес-проект[129];

2) эмиссия токенов[130] (release of tokens), как правило, включает два этапа:

а) предварительная продажа, которая предполагает предоставление скидки на покупку токенов;

б) продажа токенов по полной цене;

3) листинг токенов (token listing) – размещение токенов на одной или нескольких биржах[131].

Отсутствие нормативных актов, регламентирующих ICO, позволяет стартапам привлекать большие объемы финансирования с минимальными усилиями, избегая при этом затрат на соблюдение требований и посредников, что приводит к высокому инвестиционному риску [586, 694]. Более того, отсутствие обязательного раскрытия информации позволяет заемщикам не предоставлять информацию о платформе, что приводит к отсутствию прозрачности на рынке ICO [697].

Согласно данным CoinSchedule, в 2017 году состоялось 366 ICO, которые в совокупности привлекли 6,2 млрд долларов. По состоянию на сентябрь 2018 года, проведены 1178 ICO[132] с общим объемом финансирования 25,1 млрд долларов [694]. Вместе с тем следует отметить высокую асимметрию ICO: на десять крупнейших выпусков пришлось 13,7 млрд долларов[133]. Данные о привлеченных

---

[129] В техническом документе представлена техническая информация о продукте, подлежащем разработке, и о правах на токен, а также описана дорожная карта развития компании или стартапа.

[130] Как правило, осуществляется с использованием механизма смарт-контракта, код которого общедоступен.

[131] В ICO цена предложения определяется самой компанией и курсом криптовалюты. Фундаментальная ценность токена заключается в его функциональности и полезности. Удовлетворение инвесторов ценой предложения отражается в ставке привлечения средств на стадии массового сбыта. Торговые цены бирж криптовалюты, определяемые по заявкам на покупку и продажу в системе аукциона, аналогичны торговым ценам бирж ценных бумаг [586].

[132] С января 2016 года (первая запись).

[133] К ним относятся EOS, которая провела ICO, собравшая 4,2 млрд долларов США в июне 2018 года, и Telegram, которая развивает службу обмена сообщениями на основе Блокчейн, привлеклшая 1,7 млрд долларов США в ходе предварительной продажи в марте 2018 года.

инвестициях с использованием представленных механизмов с июля 2019 года – по июль 2020 года свидетельствуют о положительной динамике роста и достижении суммарного объема привлеченных инвестиций в размере 26,24 млрд долларов в июле 2020 года [698].

Вторичный рынок криптовалют позволяет осуществлять перепродажу ранее приобретенных криптовалют (токенов) за фиатные деньги, криптовалюты или другие активы посредством таких FinTech институтов, как биржевые платформы[134]. Биржи также предоставляют различные финансовые продукты, связанные с криптовалютой, такие как фьючерсы и опционы.

Анализ показывает, что по сравнению с другими каналами финансирования ICO имеют на первичном рынке признаки краудфандинга в том, что предоставляют заинтересованным ранние инвестиционные возможности, и признаки IPO в том, что обеспечивают ликвидность вторичного рынка.

Среди криптовалют первой децентрализованной валютой, выпущенной частным образом в 2009 году, является Биткойн [692]. Стремительный рост интереса к Биткойну на первоначальном этапе, по мнению ряда исследователей, обусловлен растущим недоверием населения к существующей финансовой системе (включая ненадлежащее государственное регулирование, сложные финансовые продукты и рискованное поведение инвестиционных банков) в результате последствий финансового кризиса 2007–2008 годов[135] [699].

Важно отметить, что Биткойн, как FinTech-институт, представляет собой также систему электронных денежных переводов, которая позволяет переводить деньги между физическими лицами. Таким образом, Биткойн имеет двойственную природу, выступая как в качестве валюты[136], так и в качестве платежной сети [700].

Биткойны, как правило, хранятся в цифровых кошельках, поэтому у пользователя должен быть доступный кошелек для покупки и продажи Биткойнов. В кошельке хранятся личные ключи, которые используются для доступа к адресам Биткойна и подписания

---

[134] Биткойн впервые стал публично торговаться на онлайн-биржах криптовалюты в 2010 году.

[135] Рейтинг доверия к органам власти в данный период был на рекордно низком уровне – составлял 17% (Trust in Government Nears Record Low, But Most Federal Agencies Are Viewed Favorably. – Режим доступа: http://www.people- press. org/2013/10/18/trust-in-government-interactive/. – Дата доступа: 4.04.2020).

[136] Согласно экономической теории, валюта имеет три основных свойства – это средство обмена, единица стоимости и накопитель стоимости.

транзакций. Существуют различные типы кошельков Биткойна, включая настольные, мобильные, веб- и аппаратные кошельки[137][692]. По данным coinmarketcap.com (от 25.01.2021), рыночная капитализация Биткойна составляет 627,4 млрд. долларов, с долей рынка 62,4%.

В 2014 году совместно с первичной продажей криптовалюты Эфира (ETH) запущена платформа Блокчейна – Ethereum [138] [678]. Данная платформа предназначена для следующих приложений: 1) финансовых (валюты, системы токенов); 2) инвестиционных (краудфандинг); 3) нефинансовых (онлайн-голосование, децентрализованное управление). В Ethereum узлы проверяют блоки (составленные из транзакций) в обмен на вознаграждения (единицей криптовалюты является Эфир) [275, 701]. По данным coinmarketcap.com (от 25.01.2021), рыночная капитализация Ethereum составляет 157,7 млрд долларов с долей рынка 16,51%.

Особенностью данной Блокчейн-платформы является реализация концепции смарт-контрактов. Использование FinTech института смарт-контрактов в финансовой сфере позволяет повысить

---

[137] Биткойн-кошельки – это программные приложения, которые облегчают процесс покупки, продажи и управления Биткойнами. Приложение кошелька может быть загружено в терминал пользователя (компьютер или смартфон) или размещено провайдером в облаке. Некоторые игроки, ориентированные на развивающиеся рынки, такие как Kipochi и BitPesa, разрабатывают «облегченные хостинговые кошельки» с интерфейсами SMS, USSD и HTML5. До сих пор ни один сервис на основе Биткойнов не был успешно интегрирован в ранее существовавший сервис мобильных денег. Типы элементов удобства клиентов, представленные кошельками, включают: 1) возможность отправлять Биткойны на адреса электронной почты, а не на адреса Биткойнов; 2) возможности генерации и сканирования QR-кода для удобного обмена Биткойн-адресами; 3) интеграция с биржами, так что транзакции могут быть выражены в Биткойнах или национальной валюте; 4) различные инструменты построения графиков и аналитики для просмотра истории Биткойнов. Кроме того, облачные кошельки имеют дополнительные преимущества: а) кошелек доступен с любого устройства через процедуру безопасного входа в систему; б) все проверки Биткойнов выполняются провайдером в облаке, поэтому пользователям нет необходимости загружать большие файлы Блокчейнов на свои устройства; 3) входящий Биткойн может быть принят провайдером кошелька в облаке, даже если пользователь находится в автономном режиме, он может быть уведомлен об этом факте по заранее заданным каналам связи.

[138] 60 млн простых Эфиров были предоставлены авторам предварительной продажи, а 12 млн простых Эфиров – разработчикам валюты и Ethereum Foundation. Торговля валютой началась в августе 2015 года, после чего майнинг валюты достиг скорости 5–8 Эфиров каждые 15–17 с для нового годового предложения, теоретически варьирующегося от 9,3 до 16,8 млн Эфиров.

эффективность обмена активов без необходимости посредника[139] [667]. Так, смарт-контракты дают возможность снизить финансовые риски, сократить расходы на администрирование и обслуживание и повысить общую эффективность финансовых услуг [266]. Среди перспективных направлений использования данной технологии в финансовой сфере выделяют следующие:

а) рынки капитала и инвестиционный банкинг. Смарт-контракты позволяют значительно сократить расчетный период (с 20 и более дней – до 6–10 дней), что повышает привлекательность для клиентов [702];

б) коммерческие и розничные продажи. Смарт-контракты могут потенциально снизить затраты и задержки за счет автоматизации процессов ипотеки с оцифровкой юридических документов в Блокчейн [288];

в) страхование. Применение смарт-контрактов в страховой отрасли также может снизить накладные расходы на обработку и сэкономить затраты, особенно при анализе претензий [703].

Важно отметить, что высокая волатильность цен на Биткойн и Эфир делает их непригодными для широкого использования в качестве обычных платежных средств. Инновации в виде стейблкоинов, стоимость которых привязана к эталонным активам, таким как фиатные валюты, рассматриваются как следующий шаг для использования данных криптовалют в качестве расчетных единиц. Общее определение данного класса криптоактивов отсутствует. Согласно определению Энт, Фидлера, Стреляя, стейблкоины – это токены на основе Блокчейн с ограниченным ценовым риском [704]. Мойн, Секники, Сирер характеризуют стейблкоины как класс криптоактивов, созданный с целью обеспечения стабильности, необходимой для функционирования денег. Как следует из названия, они предназначены для обеспечения стабильности цены относительно некоторого контрольного актива, такого, например, как доллар США [705].

---

[139] Токен – это код, который представляет собой взаимозаменяемые товары для торговли, и это могут быть «монеты, акции, результаты или билеты, или все остальное, что можно передавать и считать». Функция токенов зависит от требований контракта, но некоторые платформы имеют определенное применение для токенов [264]. В платформе Ethereum есть токены, которые можно использовать для оплаты каждой транзакции (токена использования), и токены, которые определяют участие или владение контрактом (рабочие жетоны) (What is An Ethereum Token: The Ultimate Beginner's Guide. – Режим доступа: https://blockgeeks.com/guides/ethereum- token/. – Дата доступа: 03.03.2021).

По мнению Е. Л. Сидоренко, стейблкоины являются инструментом хеджирования рисков децентрализованных монет, призванным минимизировать риски инвесторов при обороте цифровых активов без вывода средств на банковский фиатный счет [706].

Классификация стейблкоинов, согласно трекинговой платформе CoinGecko, представляет собой следующий вид [707]:

1) обеспеченные (фиатными активами), например USDT, USDC;

2) с чрезмерным обеспечением (криптовалютными активами), например DAI, sUSD;

3) алгоритмические стейблкоины, детерминированно (то есть с помощью алгоритма) регулирующие свое предложение с целью приближения цены криптовалюты к целевой цене:

а) перемещаемые алгоритмические стейблкоины, меняют предложение криптовалюты пропорционально для всех держателей токенов в соответствии со спросом (например, Ampleforth (AMPL);

б) сеньоражные алгоритмические стейблкоины[140]:

– одиночные токены (Empty Set Dollar (ESD);

– двойные токены (Basis Cash (BAC) Basis Share (BAS);

– фракционные (Frax (FRAX) Frax Share (FXS).

Классификация, используемая компанией ConsenSys Codefi, предполагает выделение следующих групп стейблкоинов: обеспеченные фиатными активами, обеспеченные криптовалютными активами, прибыльные, синтетические, алгоритмические [648].

Наиболее популярным стейблкоином является Tether, стоимость которого всегда соответствует стоимости доллара США[141]. По данным coinmarketcap.com (от 25.01.2021), рыночная капитализация Tether (USDT) составляет 24,9 млрд долларов, с долей рынка 2,58%. На Tether приходится 76% капитализации стейблкоинов.

По данным трекинговой платформы CoinGecko, объем стейблкоинов в 2020 году увеличился на 440% и приблизился к 30 млрд долларов. Лидерами роста стали USDT, USDC, DAI, BUSD и PAX, а наибольший рост в относительном выражении показал DAI – 2700% [707].

---

[140] Система Сэмса состоит из двух токенов: самой валюты с эластичным предложением и инвестиционных «долей» сети. Владельцы последнего актива, который Сэмс называет «сеньоражными акциями», являются единственными получателями инфляционных доходов от положительного увеличения предложения и единственными носителями долгового бремени, когда спрос на валюту падает и сеть сокращается.

[141] Tether был запущен в 2014 году. Идея заключалась в создании стабильной криптовалюты, которую можно было бы использовать в качестве цифрового доллара или «стейблкоина». Торговля Tether была начата 25.02.2015.

Криптовалюта Polkadot эмитирована швейцарским фондом Web3 Foundation, основанным с целью реализации проекта по созданию функциональной децентрализованной сети. Блокчейн Polkadot разработан в октябре 2017 года для интеграции частного Блокчейн (консорциумов), публичных Блокчейн-сетей без разрешений, оракулов и будущих технологических разработок, которые еще предстоит разработать в Web3. По данным coinmarketcap.com (от 25.01.2021), рыночная капитализация Polkadot (DOT) составляет 16,0 млрд долларов с долей рынка 1,69%.

Пятое место среди наиболее популярных криптовалют занимает Ripple, созданная в 2012 году с целью обеспечения безопасных, мгновенных, дешевых глобальных финансовых транзакций [254]. Главное отличие Ripple от других криптовалютных проектов заключается в целевых участниках – финансовых учреждениях[142]. В сети Ripple участвуют 12 из 50 крупнейших банков мира, включая Santander, BBVA и Standard Chartered [708]. Концептуально Ripple является одновременно стандартным представлением о криптовалютах как платежной системе в реальном времени и новым классом финансовой сети[143].

По данным coinmarketcap.com (от 25.01.2021), рыночная капитализация Ripple[144] (XRP) составляет 12,4 млрд долларов с долей рынка 1,29%.

---

[142] Ripple широко используется банками в качестве технологии расчетной инфраструктуры, поскольку он соединяет банки, провайдеров платежей, биржи цифровых активов и корпорации через RippleNet, в то время как его целью является повышение скорости финансовых транзакций, и главным образом международных банковских транзакций, с платежами, проводимыми всего за четыре секунды. Ripple можно использовать в качестве промежуточной валюты для расчетов в режиме реального времени, что позволяет эффективно осуществлять трансграничные платежи для финансовых учреждений [679].

[143] Ripple, возможно, станет преемником SWIFT, нынешней глобальной платежной системы, используемой финансовыми учреждениями. Ripple-транзакции автоматически передаются через открытые узлы в сети к месту назначения, зачисляя и дебетуя промежуточные узлы кошелька, не требуя вмешательства человека. Структура сети Ripple состоит из шлюзов, маркет-мейкеров и пользователей. Шлюз – это бизнес-кошелек (например, Standard Chartered Bank), который может аутентифицировать и загружать кредитные ссылки на новые кошельки, желающие присоединиться к сети. Шлюзы являются аналогами Ripple коммерческих банков и кредитных агентств в традиционной кредитной модели. Вновь созданный кошелек Ripple, не имеющий доверительных отношений с другими кошельками, может создать кредитную ссылку на шлюз и через эти отношения взаимодействовать с остальной частью сети, прежде чем создавать прямые ссылки на другие кошельки. Шлюзы могут применять процесс проверки подлинности с использованием известных идентификаторов в целях регулирования (например, соответствие KYC/ПОД-ФТ) и для снижения риска.

[144] Торговля Ripple началась 04.08.2013.

Отдельного внимания заслуживают проекты экосреды децентрализованных финансов (DeFi), обобщающего термина для всего спектра финансовой деятельности через Блокчейн, направленного на автоматизацию финансового сектора[145] [673]. Это приложения, биржи, сервисы для выдачи кредитов и открытия вкладов и пр.[146] Многие DeFi-проекты обладают собственной криптовалютой, преимущественно выпущенной на Блокчейн Ethereum [709].

По данным трекинговой платформы CoinGecko, DeFi-токены в 2020 году выросли в среднем на 700%, их доля в капитализации рынка с июня по август 2020 года увеличилась от 0,9% до 4,6%, а капитализация на максимуме – в 12 раз (до 19,6 млрд долларов). Доходность DeFi-токенов при этом в некоторых случаях приближалась к 3000%, а средняя составила 718% [707].

К концу 2020 года объем средств, заблокированных на рынке DeFi, составил 15,34 млрд долларов [710]. С октября по декабрь 2020 года данный показатель вырос на 37% по сравнению с предыдущим кварталом. Лидером рынка стала платформа Maker. По состоянию на 13 января 2021 года объем заблокированных на ней средств составил 3,93 млрд долларов. Второе место занимает Aave, на третью позицию опустилась децентрализованная биржа Uniswap. Наибольшая доля средств в DeFi-сервисах приходится на займы – они составляют 46% от общего объема рынка. Следом идут децентрализованные биржи (32%) и деривативы (12%).

Важно отметить тенденцию сближения характеристик рынка криптовалют и традиционного рынка ценных бумаг. Так, Чикагская биржа опционов (CBOE) и Чикагская товарная биржа (CME) в декабре 2017 года осуществили запуск торговли криптовалютными деривативами – фьючерсами на Биткойны[147] [711], в феврале 2021 года – фьючерсами на Эфир [712]. Данные об объемах торговли фьючерсами CME в июне 2020 года имеют волнообразный характер и колеблются от 100 млн долларов до 800 млн долларов в день [698].

---

[145] Например, пользователи могут внести цифровой актив в смарт-контракт в качестве обеспечения ссуды другого цифрового актива. Развиваются и другие децентрализованные финансовые услуги, такие как торговля, кредитование, инвестиции, управление активами и страхование.

[146] Ключевая идея таких платформ – отсутствие контроля разработчиков над средствами пользователей. Самой популярной децентрализованной площадкой сейчас является Uniswap.

[147] В январе 2020 г. CME запустила опционы на фьючерсные контракты BTC.

В сентябре 2019 года криптовалютная платформа Bakkt запустила фьючерсный инструмент на Биткоин [713]. Данные об объемах торговли фьючерсами Bakkt в июне 2020 года колебались в диапазоне от 16 млн долларов до 41 млн долларов в день [698].

Торговля фьючерсами на основных специализированных криптовалютных биржах, по состоянию на 08.07.2020, достигла на Huobi 1500 млн долларов в день, OKEx – 1300 млн долларов, Binance – 1250 млн долларов [698].

Важно отметить, что в 2021 году представители компании BlackRock[148] подали заявку в Комиссию по ценным бумагам и биржам США (SEC) на добавление Bitcoin-фьючерсов в список активов для инвестирования. Участие этого инвестиционного гиганта в криптовалютных операциях придаст дополнительную динамику криптовалютному рынку, а также привлечет новых корпоративных инвесторов на данный рынок.

Более того, компания S&P Dow Jones Indices объявила о планах запустить «глобальные индексы на криптоактивы» в 2021 году [714]. Создание нового инструментария для криптовалютного рынка может стать мощнейшим толчком для его дальнейшего развития. Запуск криптовалютных индексов от S&P Dow Jones Indices также создаст основу для формирования индексных фондов (ETF) на базе Биткойна, инвесторами которых являются крупнейшие игроки финансового рынка[149].

По состоянию на конец 2020 года, свыше 7000 криптовалют участвуют в торгах на более чем 20 000 онлайн-биржах. Их общая рыночная капитализация превысила 1 трлн долларов.

По данным трекинговой платформы CoinGecko, криптовалюты из топ-30 в 2020 году выросли в среднем на 300%, существенно превзойдя значения 2019 года, когда рост составил 68 млрд долларов, или 62%. Показатель роста Эфира составил за 2020 год –

---

[148] BlackRock – крупнейшая в мире инвесткомпания. На конец 2020 года она управляла активами на 8 трлн долларов. BlackRock изучала возможность инвестиций в Биткойн-фьючерсы в 2018 году, но тогда пришла к выводу, что рынок криптовалют недостаточно зрелый и ему не хватает легитимности.

[149] ETF являются самым популярным типом индексных фондов как среди индивидуальных, так и среди институциональных инвесторов. Рынок ETF сравним с рынком акций: в ноябре стоимость активов под управлением биржевых фондов в США превысила 5 трлн долларов. Три крупнейшие компании США по объему активов в управлении – BlackRock, Vanguard и State Street (так называемая «Большая тройка») – владеют 80% всего объема индексных фондов страны.

472%, Биткойна – 303%. В результате доля Ethereum на рынке увеличилась на 3,6% (до 11,5%), а Биткойна – на 0,9% (до 73,7%) [707].

По мнению аналитиков CoinGecko, высокая динамика рынка криптовалют в 2020 году обусловлена такими факторами, как [707]:

1) рост доступности криптовалютных инвестиций;

2) меры фискального стимулирования и инфляция;

3) увеличение участия институциональных инвесторов.

Одной из ключевых современных концепций цифровизации экономики является E-Government («цифровое правительство»)[150]. Данная концепция описывает реформирование государственного управления и системного предоставления цифровых услуг [221]. E-Government – обобщающий термин, охватывающий электронное правительство, электронное управление, цифровое правительство, единое правительство и онлайн-правительство [537]. К основным составляющим E-Government следует отнести: определение общих принципов предоставления услуг цифрового правительства; модульность построения; навыки управления цифровым инструментарием E-Government; измеримость.

Корси и Норрис [715] предложили следующую эволюцию данной концепции. Первый этап – присутствие государственных органов управления в Интернете, где предоставляется такая информация, как описание функций, предлагаемых органами государственного управления, имена ответственных должностных лиц, контактные данные (E-Government 1.0). Второй этап – интерактивный, предполагающий следующее взаимодействие: предоставление форумов для публикации сообщений (двусторонняя связь) либо размещение административных форм онлайн (E-Government 2.0). Третий этап – транзакционный, на котором административные процессы могут проводиться в режиме онлайн: подача налоговых деклараций онлайн, продление регистрационных процедур, получение справок и выписок (E-Government 3.0). Предполагается интеграция информации, процессов, учреждений и физической инфраструктуры с целью улучшения качества обслуживания граждан и юридических лиц в сложных условиях высокой динамики воздействия внешних и внутренних факторов [716]. Концепция предполагает преобразование разрозненных государственных служб в

[150] Концепция берет начало с Датского центрального реестра граждан (Danish Central Citizen Registry), который был разработан и внедрен в конце 1960-х годов как один из первых центральных хранилищ информации о гражданах в мире [717].

E-Government 3.0 [718, 719], ориентированное на граждан и эффективное предоставление услуг на основе гибкой экосистемы открытых данных [720].

Четвертый этап – реинжиниринг процессов, взаимосвязанных баз данных, находящихся в разных бюро, цифровой идентификации (E-Government 4.0). Последних два этапа требуют системной оцифровки процессов, необходимых для выполнения конкретных социальных функций до такой степени, что не требуется человеческое вмешательство в процессы на стороне поставщика социальных функций. В перспективе результативность цифрового правительства (E-Government 4.0) в значительной степени будет зависеть от разработки и использования динамических возможностей с поддержкой IoT для стимулирования, дальнейшего развития и ускорения процесса цифровой трансформации государственного регулирования [221]. Важнейшими составляющими эффективной системы государственного регулирования являются политики кибербезопасности IoT и развития цифровых технологий, направленных на реализацию государственных инициатив и программ по цифровизации и оцифровке данных. Эти две составляющие государственной политики рассматриваются как дополняющие друг друга, а не как заменители. E-Government 4.0 предполагает также интеграцию с такими службами, как геопространственная информация, нормативные публикации и документы для общественных обсуждений [532].

Концепция Smart government («умного правительства») была предложена как адаптивная эволюция концепции E-Government для расширения инноваций по таким направлениям, как вовлеченность граждан, подотчетность органов государственного управления и эффективность взаимодействия по линии граждане – государство – предприятия [721, 722]. Внедрение цифрового правительства, как показывает практика, способствует снижению коррупции среди государственных служащих [723].

Следует учитывать влияние на системы E-Government технологий Блокчейн и AI [532]. Так, смарт-контракты меняют управление государственным сектором, в том числе посредством формирования возможности заключения публичных тендерных контрактов, автоматизации торгов, поддержки функций контроля и аудита [266]. Таким образом, Блокчейн может существенно предотвратить мошенничество с данными и обеспечить прозрачность публичной информации.

Технологии AI, такие как ML, обработка естественного языка и распознавание речи, при условии их интеграции в государственном секторе, несут важные последствия для многих аспектов деятельности государства, включая бизнес-процессы правительственных учреждений, отношения между государством и гражданами, а также роль государства как регулятора [724]. Двиверди предложил использовать преимущества дальнейшей интеграции AI и цифрового правительства для решения задач предоставления государственных услуг, адаптированных к индивидуальным потребностям граждан [321].

1. «Умный сервис» сократит сроки и стоимость предоставления услуг, в том числе за счет оптимизации бизнес-процессов. Автономные системы и интеллектуальные чат-боты получат возможность предоставлять услуги круглосуточно, без выходных, государство – дополнительно оптимизировать количество государственных служащих и более эффективно использовать данный ресурс.

2. Интеллектуальные адаптивные формы позволят обеспечить 100%-ные индивидуализированные услуги для каждого гражданина или юридического лица за счет вычислительного потенциала AI.

3. Запрограммированные услуги предоставляются физическим и юридическим лицам без необходимости подачи предварительной заявки.

Виртц, Вейер, Гейер сосредоточились на проблемах внедрения AI в государственном управлении, сделав вывод о необходимости совершенствования законодательства и нормативных актов в области AI для контроля над управлением, включая автономные системы разведки, ответственность, а также конфиденциальность (безопасность) [728].

Заключение

Таким образом, проведенный анализ современных концепций цифровизации позволяет предложить авторскую концепцию Новой экономики 2.0, для которой характерна конвергенция взаимосвязанных цифровых технологий, выраженная в развитии новых цифровых концепций, определяющих развитие конкретных отраслей и направлений экономики, формирующих новую экономическую среду в условиях глобализации, транснационализации и НИОКР.

Концепция Новой экономики 2.0 предполагает развитие следующих направлений в их комплементарности: цифровизация традиционных отраслей экономики; реализация новых отраслевых цифровых концепций как на уровне отдельных предприятий, так и отраслей; внедрение нового цифрового инструментария в финансовых секторах как на уровне финансовых институтов, так и регуляторов; внедрение цифровых систем государственного управления.

Синергия данных изменений требует принятия соответствующих мер на уровне государства с целью адаптации «старой экономики» и минимизации рисков (адаптивный подход). Для проактивного подхода характерно принятие средне- и долгосрочных программ и проектов на уровне государства, предполагающего системный комплексный подход при их разработке и внедрении с учетом комплементарности направлений цифровизации с целью задания вектора развития страны и повышения конкурентоспособности экономики, а также учетом имеющихся страновых преимуществ, эндогенных и экзогенных условий и факторов.

Глава 2

УГРОЗЫ И РИСКИ ЦИФРОВИЗАЦИИ ЭКОНОМИКИ ДЛЯ НАЦИОНАЛЬНОЙ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

В условиях высокой динамики внедрения цифровых технологий в традиционных отраслях, а также формирования новых цифровых сегментов осуществляется интенсивная трансформация технологических, управленческих и бизнес-подходов в современной экономике. В данном контексте значительно вырастают риски, связанные не только со стабильным развитием макро- и микроэкономических систем в цифровой экосистеме, но и их уязвимостью в условиях роста кибератак, угроз национальной безопасности в сфере критической инфраструктуры и пр. Представляется важным выделить риски, связанные с цифровизацией экономики, классифицировать их по степени вероятности и потенциалу возможного ущерба как на уровне предприятия, так и страны в целом, а также рассмотреть наиболее эффективные механизмы управления цифровыми рисками.

2.1. Концептуально-аналитические подходы к возникновению потенциальных угроз в цифровой экономике и методология управления

Разработка эффективных механизмов прогнозирования потенциальных угроз цифровизации различных сфер экономики является важнейшей задачей, позволяющей в дальнейшем оптимизировать финансовые, людские и технологические ресурсы предприятия (страны, интеграционной группировки, международного сообщества) для управления рисками с целью нивелирования возможного ущерба киберугроз и восстановления стабильного развития экономических систем на различных уровнях в максимально короткие сроки. По данным отчета о глобальных рисках в 2022 году [726] отмечено, что на региональном уровне «угрозы кибербезопасности» входят в пятерку основных рисков в Восточной Азии и Тихоокеанском регионе, а также в Европе. Многие небольшие экономики

с высоким уровнем цифровизации, такие как Дания, Израиль, Япония, Тайвань (Китай), Сингапур и Объединенные Арабские Эмираты, также поставили этот риск в пятерку основных опасений. Четыре страны – Австралия, Великобритания, Ирландия и Новая Зеландия – поставили его на первое место.

Следует отметить, что концепция риска претерпела несколько трансформаций[1] и в настоящее время отражает ряд контекстов, включая предпринимательский, социальный, экономический, безопасности, инвестиционный, военный, политический и т. д. [727].

На международном уровне принят стандарт ISO 31000, который характеризует риск как влияние неопределенности на цели и выражается в виде сочетания последствий события (включая изменение обстоятельств) и связанной с этим вероятности возникновения [432, 728]. Согласно классическому определению Британского института стандартов, риск рассчитывается как «комбинация вероятности или частоты возникновения определенной опасности и величины последствий этого события» [729].

Международный совет по управлению рисками (IRGC) выделяет риски системного характера, которые обычно охватывают более одной страны, более одного сектора экономики и могут оказывать влияние на природные, технологические и социальные системы [432, 730]. Эти риски могут быть относительно редкими по вероятности наступления, но иметь глубокие последствия для безопасности, экономической и социальной стабильности. В этой связи IRGC различает три категории возникающих рисков, связанных с технологиями: а) неопределенного воздействия; б) системного воздействия; в) неожиданного воздействия [731].

Руан [727] риски управления на уровне предприятия (ERM) рассматривает как в микроэкономическом, так и макроэкономическом

[1] Концепция риска возникла в XVII веке с математикой, связанной с азартными играми. Риск относится к комбинации между вероятностью и величиной потенциальных прибылей и убытков. В XVIII веке риск как нейтральная концепция все еще рассматривался как выгоды, так и убытки и использовался в бизнесе морского страхования. Риск в изучении экономики возник в XIX веке. Понятие риска, которое в настоящее время воспринимается более негативно, заставило предпринимателей требовать специальных стимулов для принятия риска, связанного с инвестициями. К XX веку, когда речь шла о результатах риска в технике и науке, была сделана полная отрицательная коннотация, особенно в отношении опасностей, связанных с современными технологическими разработками, такими как нефтехимическая и атомная промышленность (The Royal Society, 1992).

разрезах, выделяя следующие их разновидности: стратегический, кредитный, операционный, регуляторный, рыночный и системный.

Ряд исследователей [732] выделяет эндогенные и экзогенные риски на уровне ERM. К эндогенным рискам относятся:

1) риски, связанные с организационной сетью, включая любые неопределенности, возникающие в результате взаимодействия между организациями в рамках бизнес-экосистемы;

2) риски, связанные с бизнес-процессами, такими как сбои во внутренних операциях (продукт (услуга), процесс (контроль)), материальный, финансовый и информационный потоки, а также риски, связанные с принятием решений;

3) риски, связанные с цепочкой поставок, включая риски со стороны предложения (спроса), такие как банкротство поставщика, сбои распределенных или транспортных поставщиков и т. д.;

4) риски, связанные с безопасностью, включая злонамеренные угрозы (преднамеренные и непреднамеренные, такие как кража, саботаж, промышленный шпионаж, кибератака и т. д., а также сбои в инфраструктуре, включая IT, и финансовые риски.

Экзогенные риски классифицируются:

1) на риски, связанные с окружающей средой в целом, которые возникают в результате взаимодействия бизнес-экосистемы с окружающей средой;

2) стихийные бедствия, такие как эпидемические заболевания, ураганы, наводнения, торнадо и т. д.;

3) социально-экономические риски, такие как политические (эмбарго, война, терроризм и т. д.), экономические (рецессия, колебания валютных курсов, высокие банковские интересы и нехватка средств и т. д.) и политические (регулирующие, правовые и бюрократические);

4) инфраструктурные риски, включая глобальные сбои инфраструктуры, такие как Интернет, электрические сети и т. д.

С учетом растущего внимания к преступлениям в сфере IT сформировано понятие «киберпреступление». Киберпреступность можно определить как компьютерные и информационно-технологические правонарушения, которые включают несанкционированный доступ к пользовательским данным, изменение или нарушение электронных коммуникаций с использованием указанных данных для личной выгоды или получения финансовой выгоды [733].

Киберпреступления имеют как краткосрочные[2], так и долгосрочные[3] последствия [733, 733]. По мнению правоохранительных органов Великобритании, современная киберпреступность является одной из самых серьезных угроз экономическому благополучию страны [736].

Термин «киберриск» NIST определяет как «риск, возникающий из-за потери конфиденциальности, целостности или доступности информации или информационных систем и отражающие потенциальные неблагоприятные воздействия на деятельность организации (например, миссию, функции, имидж или репутацию), активы организации, отдельных лиц, другие организации и страну» [737].

Ключевые компоненты киберриска, согласно NIST, включают:

1) угрозы – это любые обстоятельства или события, которые могут оказать неблагоприятное воздействие на деятельность и активы организации, отдельных лиц, другие организации или нацию через несанкционированный доступ к информационной системе, уничтожение, разглашение или изменение информации и (или) отказ в обслуживании (DoS);

2) уязвимости – это слабость информационной системы, процедур безопасности системы, внутреннего контроля или реализации, которые могут быть использованы источником угрозы;

3) вероятность возникновения – это взвешенный фактор риска, основанный на анализе вероятности того, что данная угроза способна использовать данную уязвимость (или набор уязвимостей).

На микроэкономическом уровне киберриски являются важной составляющей стратегического риска предприятия, кредитного риска, а также регуляторного риска[4] [727]. Кибератаки на частный сектор становятся все более важным риском в анализе корпоративного кредитования [738]. Более того, рейтинги кибербезопасности компаний учитываются при оценке инвестиций [739].

---

[2] Краткосрочные последствия – это когда значительные ежедневные финансовые и другие потери затрагивают ежедневную деятельность предприятий и правительств.

[3] Утрата репутации может быть отнесена к долгосрочным последствиям. Например, в 2018 году утечка данных, затронувшая 50 млн пользователей Facebook, вызвала потерю доверия инвесторов к Facebook и потерю около 43 млрд долларов капитализации.

[4] Согласно оценкам, из-за успешной атаки 60% предприятий малого и среднего бизнеса прекращают свою деятельность в течение 6-месячного периода. Конкурентные преимущества или коммерческие секреты часто являются основными целями кибератак. Исследование показывает, что каждый пятый бизнес, пострадавший от вымогателей, вынужден закрыться.

На макроэкономическом уровне киберриск может явно влиять на рынки и представлять системный риск, генерируя вероятность разрушения системы или рынка.

В данном контексте актуальной представляется проблематика управления рисками как на уровне государства, так и отрасли или предприятия. Анализ рисков, в соответствии с определением Общества по анализу рисков (SRA), – это отдельная наука, охватывающая оценку рисков, восприятие, коммуникацию, управление, руководство и политику в контексте рисков, вызывающих озабоченность отдельных лиц, организаций государственного и частного секторов и общества на местном, региональном, национальном или глобальном уровне, это применение принципов управления для идентификации, оценки, управления и передачи риска [453, 740]. Управление рисками включает в себя совокупность действующих лиц, правил, соглашений, процессов и механизмов, связанных с тем, как собирается, анализируется и распространяется соответствующая информация о рисках и принимаются управленческие решения. Управление рисками лежит в основе глобальной финансовой системы, работы ее международных рынков капитала, транснациональных, региональных и местных игроков, а также основных продуктов и услуг [559].

Международный совет по управлению рисками (IRGC) разработал интегрированную аналитическую основу для управления рисками, которая обеспечивает руководство для формирования комплексных стратегий оценки и управления рисками, в том числе на глобальном уровне [741]. Данная структура разделена на три основных этапа: предварительная оценка, окончательная оценка и управление.

Рамезани и Камаринья-Матос отмечают необходимость компаниям, управляющим крупными, глобальными, конкурентными и сложными цепочками, использовать подходы для проактивного и реактивного противодействия различным угрозам [732]. В этой связи предложен механизм трехэтапного управления рисками: подготовка, реагирование и восстановление:

1) этап подготовки предполагает комплекс упреждающих мер и действий по выявлению и устранению источника возможных сбоев или снижению (смягчению) их негативного воздействия. Кроме того, вводят другие важные стратегии для этой фазы, такие как качество, эффективность, минимизация затрат, возможности хеджирования рисков, резервное копирование систем и процессов,

систематическое планирование на случай непредвиденных обстоятельств, модернизация информационных технологий и заменимость в цепочке поставок;

2) этап реагирования предполагает действия, осуществляемые за минимальный период после атаки с целью защиты имущества сообщества или бизнес-экосистемы, а также подготовку к началу этапа восстановления;

3) этап восстановления относится к действиям, направленным на возвращение системы в доаварийное или рабочее состояние за счет изменения бизнес-процессов, изучение опыта и использование новых возможностей.

Качественный скачок в управлении рисками обусловлен инновациями в технологиях, стимулируемыми беспрецедентным развитием объема и качества цифровых данных, которые становятся доступными для глобальных финансовых учреждений. Генерирование цифровых данных становится бесконечным, они регистрируются в реальном времени. Управление рисками характеризуется новыми методами прикладной аналитики и в большей степени зависит от ML/AI [559].

В условиях цифровизации актуальным является обеспечение кибербезопасности как на макро-, так и микроуровнях [727]. Кибербезопасность, согласно определению Бойсона, – «совокупность комбинированных технологий, процессов и практик, которые применяются для защиты данных и сетей от атак, повреждения или несанкционированного доступа» [742]. Большинство организаций используют одно или несколько приложений безопасности, таких как брандмауэры, антивирусное программное обеспечение или системы обнаружения вторжений [214].

Эволюция кибербезопасности в отношении процессов обнаружения вредоносного поведения, ориентированных на защиту информации в критически важных инфраструктурах и пользователей, характеризуется изменением глубины, системности и инструментария: от выявления и удаления вредоносного кода (в 2000 году) до обеспечения конфиденциальности пользователей, применения технологий Блокчейн, аналитики поведения пользователей [186].

С целью выявления наиболее эффективных механизмов снижения подверженности компании киберрискам используется анализ сценариев для оценки средств управления в случае наиболее разрушительных киберпотерь в отношении наиболее ценных цифровых

активов. Деятельность по управлению киберрисками может включать [727]:

а) построение моделей угроз и уязвимостей, направленных на выявление и классификацию угроз в разрезе их приоритетности, принятия мер по выборочному снижению рисков с наивысшим приоритетом в условиях ограниченности ресурсов организации. Данный инструмент обеспечивает аналитиков систематическим анализом профиля вероятного злоумышленника, наиболее вероятных векторов атаки и уязвимых активов. Процесс снижения рисков связан с принятием экономических решений для стратегического инвестирования ограниченных ресурсов, чтобы преобразовать неприемлемые риски в приемлемые;

б) разработку и внедрение моделей с учетом зрелости инфраструктуры, которые позволяют интегрировать различные стратегии, возможности и компоненты управления с целью повышения возможностей безопасности организации;

в) осуществление киберстрахования, позволяющего перенести риск и сократить убытки, вызванные кибернарушениями, а также дополняющего существующий набор инструментов безопасности для управления киберриском после соответствующего инвестирования. Страхование передает риск компенсируемого убытка страховщику, является стратегией [743], основанной на устойчивости[5];

г) создание нормативной базы, которая устанавливает требования к киберриску, регламентируя систему внутреннего контроля и ее мониторинга, обеспечивая тем самым целостность и правильность регулируемых активов (в т. ч. финансовых данных);

д) внедрение международных стандартов, например, таких как ISO / IEC 27000, которые содержат руководство по организации системы управления информационной безопасностью (ISMS).

Первым этапом в методологии управления рисками является его оценка, цель которой – определение степени риска и контрмеры, которые могут быть реализованы [104]. Результаты оценки риска могут быть использованы для определения переносимости или приемлемости рисков [744].

---

[5] Развивая данный подход, Фишер, Халибозек, Вальтерс предложили два альтернативных решения, которые должны дополнять друг друга: 1) инвестиции в методы предотвращения потерь и 2) страхование [746]. Вместе с тем, как показали результаты исследования «Глобальные риски в 2022 году» [726], масштабный рост кибератак привел к увеличению стоимости киберстрахования в США на 96% в третьем квартале 2021 года (204% по сравнению с показателем 2020 года).

Общепринятая методология оценки риска разработана для решения проблем безопасности и предполагает оценку потерь в расчете на вероятность наступления события[6] [745].

Вместе с тем в научной литературе при оценке безопасности выделяют два основных подхода: качественный и количественный. Количественная оценка риска – это использование измеримых, объективных данных для определения стоимости активов, вероятности потерь и связанного с ними риска (рисков) [727]. Количественные методы варьируются от ранжирования рисков, корреляций рисков, сравнительного анализа и анализа сценариев до генерации прогнозных точечных оценок, а затем до генерации прогнозных распределений (вероятностных моделей)[7]. Качественные подходы к риску, как правило, применяются к тем рискам, которые трудно определить количественно. Качественные подходы заменяют количественные значения, присваивая субъективно определенное значение, такое как высокое, среднее или низкое.

Исследовательский центр McKinsey для выявления и определения наиболее важных рисков рекомендует использовать матричную сетку рисков, где потенциальное воздействие события на всю компанию расположено по вертикальной оси, а вероятность наступления риска расположена по горизонтальной оси[8] [747]. Таким образом, потенциальные риски ранжируются по отношению друг к другу, а не по абсолютной шкале.

Вместе с тем в условиях цифровизации в современной экономике все большее распространение приобретают комплексные подходы оценки рисков, адаптированные к новым условиям и рискам.

В условиях киберугроз «оценка риска» представляет собой процесс выявления, оценки и определения приоритетов рисков

---

[6] При оценке рисков, как правило, используется формула: $R = T \cdot D$, где T – вероятность наличия опасности, а D – оценка потерь в случае повреждения системы [745].

[7] Как правило, количественные подходы следуют базовой формуле, которая идентифицирует активы, угрозы для этих активов, назначает вероятность возникновения угрозы и затем умножает эту вероятность на оценку активов. Сумма этой формулы обеспечивает базовый расчет, который учитывает вероятность потери и ее стоимость в случае ее возникновения. Многие современные количественные подходы стали сложными актуарными моделями с применением исторических данных о происшествиях для определения вероятности наступления события.

[8] Высокое размещение на вертикальной оси означает, что существование компании окажется под угрозой, если возникнет этот риск, или компания упустит огромную возможность. Низкое расположение по вертикальной оси означает, что воздействие или возможность будут ограниченными или изолированными.

информационной безопасности [104]. Оценка риска требует тщательного анализа информации об угрозах и уязвимости, чтобы определить степень, в которой обстоятельства или события могут оказать неблагоприятное воздействие на организацию, и вероятность того, что такие обстоятельства или события произойдут [737].

Разработку методов оценки рисков кибербезопасности осуществляют как международные организации, так и специализированные национальные агентства[9]. Среди наиболее распространенных является серия ISO 27000X, предполагающая непрерывный процесс структурированных последовательностей действий для организаций всех форм и размеров [748].

Некоторые из самых известных методов оценки разработаны NIST и включают платформы «800-53» и «Структуру кибербезопасности» (CSF)[10] [749]. Важно отметить, что CSF широко используется во всем мире и NIST продвигает ее в качестве «модели международного сотрудничества по укреплению критически важной инфраструктуры кибербезопасности». NIST 800-53 первоначально разработана с целью содействия компаниям в выполнении Федеральных стандартов информации США (FIPS)[11].

Национальный инфраструктурный консультативный совет США (NIAC) разработал Общую систему оценки уязвимостей (CVSS), предназначенную для осуществления открытых и универсально

[9] Наиболее широко признанными являются структуры Международной организации по стандартизации International Organisation for Standardisation ISO) и Международной электротехнической комиссии International Electrotechnical Commission (IEC), совместно ISO/IEC, а также Национального института стандартов и технологий США (National Institute of Standards and Technology NIST). Так, серия ISO 27000X предоставляет руководство по наилучшей практике для всей системы управления информационной безопасностью. Структура поощряет организации оценивать свои IT-риски, а затем вводить соответствующие средства контроля согласно их конкретным потребностям. Он включает в себя непрерывную обратную связь и мероприятия по улучшению, чтобы противостоять текущему состоянию угроз или принимать во внимание инциденты безопасности.

[10] Первая версия CSF была выпущена в 2014 году в соответствии с Законом США об усилении кибербезопасности и разработана для улучшения критической инфраструктуры кибербезопасности. Платформа содержит информацию о новых угрозах и рисках и предлагает решения путем регулярных обновлений.

[11] В эту структуру включены стратегии по приведению в соответствие Федерального закона об управлении информационной безопасностью 2002 года (Federal Information Security Management Act FISMA) с международным стандартом безопасности ISO/IEC 27001.

стандартных оценок серьезности уязвимостей программного обеспечения[12] [727].

Кроме того, на уровне компаний осуществляется использование более широкого и простого метода оценки рисков в отношении критически важных для эксплуатации, активов и уязвимостей OCTAVE[13].

Компания Microsoft разработала собственный метод оценки рисков – STRIDE, который классифицирует угрозы безопасности по 6 категориям: подмена, фальсификация, отказ, раскрытие информации, отказ в обслуживании, повышение привилегий[14] [750].

Конфиденциальность, целостность и доступность, также известная как триада «CIA», является целевой моделью безопасности, которую можно использовать в качестве общей методологии идентификации угроз[15] [751]. При этом потеря конфиденциальности,

---

[12] Он был создан как глобальная структура для раскрытия информации об уязвимостях в сфере безопасности и помогает IT-менеджерам преобразовать множество данных об уязвимостях в практические приоритеты. CVSS был принят во всем мире и используется поставщиками бюллетеней по уязвимостям, поставщиками программных приложений, организациями пользователей, компаниями по сканированию и управлению уязвимостями, фирмами по обеспечению безопасности и управлению рисками, а также исследовательскими институтами.

[13] OCTAVE был разработан в 2001 году в Университете Карнеги-Меллона (CMU) для Министерства обороны США. OCTAVE используется для определения уровней риска и для планирования против кибератак. Его структура предназначена для минимизации подверженности организаций угрозам, а также для прогнозирования вероятных результатов атак и устранения тех, которые были успешными. Структура разбита на три определенных этапа: создание профилей угроз на основе активов; выявление уязвимостей инфраструктуры; разработка стратегии и планов безопасности.

[14] *Подмена*: когда человек или программа успешно маскируется под другого, подделывая данные, чтобы получить незаконное преимущество; *фальсификация*: акт преднамеренного изменения данных по несанкционированным каналам; *отказ*: когда приложение или система не применяют элементы управления для надлежащего отслеживания и регистрации действий пользователя, что позволяет злонамеренно манипулировать или подделывать идентификацию новых действий; *раскрытие информации*: атака, такая как нарушение конфиденциальности или утечка данных, которая приводит к тому, что информационная система раскрывает конфиденциальную информацию, которая не должна раскрываться; *отказ в обслуживании*: кибератака, при которой злоумышленник пытается сделать компьютер или сетевой ресурс недоступным для своих предполагаемых пользователей путем временного или неограниченного прерывания работы хоста, подключенного к Интернету; *повышение привилегий* (Elevation of privilege EoP) – предоставление разрешения авторизации злоумышленника сверх первоначально предоставленного.

[15] Потеря конфиденциальности – несанкционированное разглашение информации. Потеря целостности – это несанкционированное изменение или уничтожение информации. Потеря доступности – это нарушение доступа или использования информации или информационной системы.

целостности и доступности может иметь низкий, средний или высокий уровень воздействия на систему.

В рамках инициативы Всемирного экономического форума «Партнерство для киберустойчивости» [752] разработана структура статистической модели для количественной оценки финансового воздействия киберугроз, в которой используется вероятность для оценки потерь от кибератак в течение заданного периода[16].

С экономической точки зрения при оценке киберрисков осуществляется оценка стоимости безопасности. В данном контексте важно отметить проблематику оценки потерь от киберинцидентов, которая обусловлена сложностью определения стоимости нематериальных цифровых активов. Следует также учитывать такой показатель, как потеря рыночной стоимости фирмы из-за сообщений о нарушениях безопасности [753][17].

Микроэкономические потери в результате киберинцендентов также могут быть определены количественно с использованием категорий убытков, включая прямые убытки, расходы на расследование инцидента и реагирование на него, репутационный ущерб, юридическую ответственность, выплату штрафов, негативное влияние на цену акций.

Следует выделить факторы, способствующие возникновению (или усилению) новых рисков, в том числе инновации, потеря запаса прочности; изменение восприимчивости к риску; конфликты интересов, социальная динамика; технический прогресс; коммуникации; информационная асимметрия; неправильные стимулы; преступные мотивы и поступки [730].

Инновационные технологии могут оказывать кардинальное влияние на производственные модели, подходы, концепции и бизнес [323]. В докладе о системных рисках, разработанном ОЭСР в 2003 году, отмечаются три аспекта новых технологий, которые влияют на риск: взаимосвязанность; скорость и распространенность технологических

---

[16] Концепция Cyber VaR основана на понятии VaR – статистическом методе, широко используемом в индустрии финансовых услуг для выражения уровня финансового риска банка (или финансового риска, связанного с конкретным инвестиционным портфелем) в течение определенного периода времени. Cyber VaR рассматривает три основных фактора киберрисков для организации: 1) уязвимость; 2) активы; 3) профиль его потенциальных злоумышленников.

[17] Cavusoglu обнаружил, что публично торгуемые взломанные фирмы в среднем потеряли приблизительно 2,1% своей рыночной стоимости в течение 2 дней, связанных с нарушениями безопасности [753].

изменений; фундаментальные изменения в среде, которые они могут вызвать [754].

Согласно Рабочему соглашению (CWA) по управлению возникающими рисками, связанными с технологией, Европейского комитета по стандартизации (CEN), определены в том числе следующие факторы, генерирующие технологические риски в промышленных организациях:

а) новые технологии;

б) новые материалы;

в) новые производственные процессы и новые производственные сети;

г) новые политики;

д) неопределенности в измерениях и характеристиках и пр. [755].

Ряд исследователей в области производственных процессов дополнительно выделяют такие факторы риска, как автоматизация и интерфейсы «человек – машина» и «человек – ИКТ» [756].

Руан классифицирует следующие факторы киберриска: технологические (связаны с использованием технологий), нетехнологические (связаны с процессами, социально-экономическими, геополитическими факторами), внутренние (основаны на характере бизнеса, отрасли, операциях, товарах и услугах и пр.), контрольные (отражают эффективность контроля предприятия в отношении кибератак и являются предметом инвестиций, когда речь идет о снижении рисков) [757].

Отмечается, что для измерения киберрисков целесообразным является создание банка данных киберрисков, с целью идентификации их ключевых факторов, связанных с профилем организации. На подверженность компании кибернетическому риску влияет широкий спектр динамических технологических и нетехнологических факторов профилирования, внутренних уязвимостей и внешних угроз. В частности, мотивы злоумышленников во многом определяются нетехнологическими факторами [758].

В контексте потенциальных рисков значительное внимание со стороны как ученых, так и практиков уделено стратегиям, разработанным для снижения рисков и эффективного реагирования на инциденты, связанные с рисками [732]. Ряд исследований рекомендует переход от управления рисками к управлению устойчивостью [759]. Это обосновывается тем фактом, что данный подход охватывает кризисные и посткризисные фазы. В этом смысле

управление устойчивостью близко к тому, что обычно понимается как кризисное управление, или цикл кризисного управления.

В научной литературе выделяют три аспекта концепции устойчивости системы:

1) способность системы восстанавливаться после сбоя и (или) атаки;

2) способность системы поддерживать желаемое состояние (то есть возвращаться к новому состоянию равновесия или принятому состоянию);

3) способность системы противостоять атаке с постепенной адаптацией и трансформацией.

Следует отметить эволюцию концепции устойчивости системы по направлению развития ее адаптивной и даже трансформирующей способности, концентрируясь на нелинейной сложности и многомерной устойчивости систем (мультиравновесия). Это означает выход за рамки традиционной устойчивости, перетаргетирование на ее улучшение и привнесение нового уровня устойчивости, формирование сложной адаптивной системы.

С экономической точки зрения при принятии управленческих решений по защите от киберугроз представляется целесообразным учитывать такие факторы, как:

1) оценка прочности элементов управления для цифровых активов;

2) измерение экономической эффективности средств управления цифровыми активами;

3) определение предела киберриска субъекта;

4) измерение стоимости снижения риска;

5) измерение рентабельности инвестиций в киберриск.

Заключение

Таким образом, следует отметить, что концепция риска претерпела ряд трансформаций и в настоящее время может рассматриваться через призму бизнеса, социальных, экономических, инвестиционных, военных и политических угроз.

Среди рисков цифровизации выделяются киберриски, которые являются важной составляющей стратегического риска на уровне предприятий, кредитного и регуляторного рисков, оказывают влияние на рынки и формируют системный риск, генерируя вероятность

разрушения элементов инфраструктуры или рынка. Риски системного характера охватывают более одной страны, более одного сектора экономики и могут оказывать влияние на природные, технологические и социальные системы.

Деятельность по управлению киберрисками включает построение моделей угроз и уязвимостей, направленных на выявление и классификацию угроз в разрезе их приоритетности, принятие мер по выборочному снижению рисков с наивысшим приоритетом в условиях ограниченности ресурсов организации. С учетом текущего состояния и эволюции киберугроз проведена сравнительная характеристика наиболее распространенных и опасных инструментов кибератак. Построена матрица рисков в зависимости от используемого инструментария киберугроз, которая позволяет выделить особо опасные с точки зрения вероятности наступления и потенциального урона киберинструменты.

2.2. Угрозы и риски цифровизации на уровне макроэкономики

Реализация цифровых концепций в рамках Новой экономики 2.0, направленных на повышение конкурентоспособности экономики в целом и отдельных ее сегментов (отраслей) в частности, неотрывно связана с нарастанием соответствующих рисков и угроз. При этом особенностью рисков на уровне макроэкономики является их системный (с возможным перерастанием в каскадный) характер и значительный потенциал генерирования соответствующего урона для экономического развития страны, критически важных секторов и сегментов экономики, социальной и общественной сферы, ее экономической безопасности. В этой связи задачей органов государственного управления является прогнозирование соответствующих рисков при планировании имплементации цифровых инноваций (реализации цифровых концепций) для национальной экономики с целью выработки соответствующих решений, направленных на нивелирование (минимизацию) цифровых угроз. Правильное выставление приоритетов регулирования, их градация с учетом вероятности угроз и масштаба урона для страны позволяют оптимизировать финансовые и человеческие затраты государства, выстроить современную систему реагирования и повысить эффективность управления данной системой по противодействию цифровым рискам и угрозам.

Поскольку макроэкономика как наука изучает поведение экономической системы в целом, охватывая сложные и взаимосвязанные отношения между домашними хозяйствами, экономическими структурами (хозяйствующими субъектами) и органами государственного управления, концепция E-Government входит в объект исследования, формируя новую цифровую инфраструктуру взаимодействия экономических агентов и государства. Кроме того, данная концепция является одной из наиболее уязвимых с точки зрения потенциала возможного ущерба государству. Важно отметить, что на внешний контур, фактически впервые в истории государственного управления, выносится широкий спектр функционала госрегулирования, что значительно повышает требования к безопасности системы, ее устойчивости к угрозам.

Органы государственного управления абсорбируют и хранят массивы персональных данных, которые являются уязвимыми для кражи данных или манипулирования [321]. Внедрение технологий E-Government создает серьезные вызовы в контексте как безопасности, так и устойчивости системы управления на макроуровне.

Важно отметить, что функционально системы E-Government выполняют три базовые операции: аккумулирование (хранение) данных, анализ данных, предоставление данных по запросу [760]. В таком контексте основными проблемами [397] E-Government являются угрозы безопасности, конфиденциальности и функциональной совместимости[18]. Потенциальные кибератаки в адрес E-Government также являются сложными и нацеленными на конечных пользователей, инфраструктуру связи и внутренние серверы[19] [761].

---

[18] Граждане зачастую не готовы взаимодействовать с электронными государственными службами из-за недостатка доверия, что является существенным барьером для широкого принятия систем электронного правительства [762].

[19] В 2015 году правительство США подверглось массированной кибератаке, в результате которой была раскрыта конфиденциальная информация около 21,5 млн сотрудников органов госуправления и членов их семей (E-government sounds great until the first hack. – Режим доступа: https://www.bloomberg.com/view/articles/2017-11-21/e-government-sounds-great-until-the-first-hack/. – Дата доступа: 13.01.2018). В результате атаки были обнаружены номера социального страхования, отпечатки пальцев, информация о кредитных картах, адреса, медицинские и финансовые записи и другая личная информация. Наряду со скоординированными атаками на системы правительства США, в Соединенных Штатах также есть случаи, когда на сайтах местного электронного правительства были доступны имена людей, номера социального страхования, данные о налогах на имущество и другая частная информация, не требующая учетных данных для входа в систему [763].

Комплексный подход к проблеме безопасности цифрового правительства предполагает выделение угроз в следующих измерениях.

1. Технологическое:

а) обеспечение стабильности системы;

б) гарантирование сохранения конфиденциальности данных.

2. Организационное:

а) актуализация информации;

б) обеспечение совместимости систем;

в) систематизация взаимодействия различных владельцев информации;

г) обеспечение документооборота цифровых документов.

3. Правовое:

а) обеспечение конфиденциальности служебной и персональной информации;

б) обеспечение циркуляции цифровых документов.

4. Экономическое: в зависимости от глубины и комплексности внедренной технологии возникает риск мультисекторальной дестабилизации[20]. Различные модели, известные как модели зрелости E-Government (eGMM), определяют направления и комплексность развития технологий цифрового правительства с точки зрения управления. Если для уровня E-Government 1.0 риски и угрозы негативного влияния нарушения стабильного функционирования системы на различные экономические сферы, социальные сектора и государственное управление являются минимальными, то для E-Government 4.0 дестабилизация системы может нанести разного рода урон на национальном уровне (табл. 2.1).

С учетом того, что на уровне макроэкономики изучаются общеэкономические явления, такие как инфляция, темпы экономического роста, национальный доход, валовой внутренний продукт (ВВП), международная торговля, международные финансы, безработица, первой по значимости и величине возможных угроз является концепция государственных цифровых валют (CBDC), которые создают существенные риски для стабильности функционирования финансовой системы государства [583].

[20] С начала реализации государственной программы Эстонии в 2014 году электронным резидентам из 174 стран было выдано около 70 тыс. цифровых удостоверений личности. По данным отчета Управления финансовой разведки полиции Эстонии, компании, возглавляемые эстонскими электронными резидентами, были причастны к «крупномасштабным мошенничествам», в том числе к организации «подозрительных ICO и незаконному присвоению крупных сумм денег». Полиция заявила, что «значительная связь» с электронными резидентами повышает риск репутационного ущерба Эстонии [764].

Таблица 2.1

Риски и угрозы E-Government в зависимости от модели зрелости
(разработано автором)

Сегмент	Модели зрелости			
	E-Government 1.0	E-Government 2.0	E-Government 3.0	E-Government 4.0
Экономическая среда	Отсутствует	Снижение качества предоставляемых экономических субъектам онлайн услуг	Дестабилизация организационных процессов; краткосрочное снижение налоговых поступлений	Финансовый ущерб экономическим субъектам и физическим лицам в случае взлома системы цифровой идентификации
Социальная среда	Отсутствует	Снижение качества предоставляемых социальных услуг населению	Рост социальной напряженности в случае продолжительного периода дисфункции системы	Дестабилизация низовых инициатив в случае взлома систем двустороннего взаимодействия граждан и правительства (например, для проведения онлайн голосования)
Государственное управление	Отсутствует	Отсутствует	Репутационный ущерб в случае кражи личных данных граждан и коммерческой информации экономических субъектов	Принятие ошибочных управленческих решений в случае взлома системы автоматического сбора цифровых данных систем IoT; экономические потери в случае невозможности заключения публичных тендерных контрактов и сбоя систем автоматизации торгов; налоговые потери в случае нарушения функционала поддержки систем контроля и аудита

Так, согласно исследованию Федеральной резервной системы США, именно риски, связанные с инфраструктурой финансового рынка, являются критически важными для устойчивости финансовой системы [717]. Типологически они включают кредитный, операционный, ликвидности и юридический риски. Эмпирический анализ позволяет отнести тенденции валютной цифровизации к операционному риску, который связан с недостатками в информационных системах или внутренних процессах, человеческими ошибками, сбоями в управлении или сбоями в результате внешних событий.

Дополнительные риски генерирует выбор определенного механизма реализации концепции CBDC. Анализ показал, что в случае использования прямой модели эмиссии и оборота CBDC может значительно ослабнуть роль коммерческих банковских учреждений с точки зрения финансовой интермедиации. Последующее сокращение банковских депозитов и снижение доходов, полученных от предоставления данной финансовой услуги, будет стимулировать увеличение процентной ставки по банковским кредитам, снижение объема кредитования и негативно повлияет на экономический рост. Так, по прогнозу экспертов Центра макроэкономического анализа и краткосрочного прогнозирования России, внедрение цифрового рубля приведет до конца 2024 года к оттоку ликвидности из российских банков 9 трлн российских руб. Нехватка ликвидности станет причиной снижения объемов банковского кредитования в размере 4–5% и сокращения прибыли банков на 10% [765]. По мнению экспертов ЕСВ [626], замещение депозитов до востребования более дорогими источниками финансирования (кредитом центрального банка или выпуском банковских облигаций) приведет к росту затрат на банковское финансирование и Центральный банк будет вынужден компенсировать данное ужесточение финансовых условий путем снижения процентной ставки в рамках денежно-кредитной политики. Ввиду того, что банковское финансирование является лишь частью общего финансирования экономики, Центральный банк не будет снижать краткосрочные процентные ставки таким образом, чтобы затраты на банковское финансирование были компенсированы только частично. Следовательно, в новом равновесии банки потеряют конкурентоспособность и некоторую долю рынка по сравнению с другими формами финансирования (через рынки капитала и небанковских посредников).

Исследование, проведенное Ассоциацией банков России в январе 2021 года, показало [766], что основной риск внедрения CBDC заключается в обеспечении безопасности криптокошельков. Несовершенная система и низкая квалификация специалистов могут стать главными факторами появления рисков для стабильности финансовой системы. Кроме этого, есть опасность появления вредоносного программного обеспечения, направленного на взлом криптокошельков и похищение денежных средств[21].

Эксперты Центра исследования финансовых технологий и цифровой экономики, созданного Московской школой управления «Сколково» и Российской экономической школой в исследовании «Цифровые валюты центральных банков: типология, дизайн и российская специфика», к основным рискам введения новой формы расчетов относят следующее [767]:

а) прямое вовлечение центральных банков в рынок финансовых услуг. Это может привести к потере регулятором роли независимого участника финансового рынка и подорвать доверие с точки зрения выполнения регуляторной функции;

б) введение CBDC может казаться слишком сложной для отдельных групп населения;

в) осуществление эмиссии CBDC центральным банком генерирует риск его конкуренции с рыночными предложениями финансовых услуг.

С учетом изложенного, Банк международных расчетов (BIS) выделяет следующие принципы построения эффективной системы CBDC [619]:

1) Центральный банк не должен ставить под угрозу денежно-кредитную или финансовую стабильность при выпуске CBDC;

2) CBDC должна сосуществовать с действующими формами денег и дополнять их;

3) CBDC должна способствовать инновациям и эффективности.

Эмитенты цифровой валюты и поставщики платежных услуг должны гарантировать устойчивость к кибератакам и, в случае кибератаки, должны быть в состоянии обеспечить быстрое восстановление и защиту целостности данных. Платежные системы должны быть устойчивыми перед лицом других внешних факторов, таких как стихийные бедствия. Одним из способов достижения этого

[21] Примером может служить использование китайской CBDC для отмывания денег группой мошенников в 2020–2021 годах.

в цифровых платежных средствах является включение функций, которые позволяют системе функционировать в автономном режиме, по крайней мере временно.

В контексте необходимости моделирования рисков и потенциально проблемных аспектов использования CBDC в финансовой системе эксперты [583] рекомендуют использование специализированных сред тестирования, таких как «нормативные песочницы» или инновационные центры, позволяющие оценить производительность, преимущества и риски, которые могут служить ориентиром для дальнейшего развития. Центральные банки и регулирующие органы обладают компетенцией разработки соответствующих правил, адаптированных к уровням риска, которые они наблюдают. В быстро меняющемся ландшафте платежей «песочницы» могут предоставить новым специалистам возможность продемонстрировать жизнеспособность лежащих в их основе технологий и бизнес-моделей, не создавая при этом несоразмерного риска. В настоящее время центральные банки и регулирующие органы более 50 стран ввели «песочницы» финансового регулирования или аналогичные инициативы[22].

Таким образом, предлагая эффективный и удобный CBDC, центральный банк может снизить риск доминирования альтернативных расчетных единиц на национальном уровне[23].

Широкое использование цифровых платежных инструментов, таких как мобильные деньги и криптовалюты, ведет к возникновению рисков финансовой дестабилизации [583].

Данные инновации могут повлиять на функционирование денежно-кредитной политики и эффективность инструментов политики центрального банка. Мобильные деньги могут по-разному влиять на денежную массу в экономике в зависимости от действующего регулирования и механизма их хранения в банковской системе. Высокая степень замещения мобильными деньгами фиатных валют или банковских депозитов может ослабить контроль центрального банка над совокупной денежной массой, увеличить скорость денежных операций, а также повлиять на доходы

[22] Первым регулирующим органом, разработавшим в 2016 году модель «песочницы», является Управление по финансовому регулированию и надзору Великобритании.

[23] Риск стейблкоинов, так называемых «криптовалют», и иностранных CBDC заключается в том, что внутренние пользователи принимают их в значительном количестве, а использование национальной суверенной валюты сокращается. В крайнем случае, такая «цифровая долларизация» может привести к замене одной национальной валюты другой, а Центральный банк страны постепенно утратит контроль над денежно-кредитными вопросами.

центральных банков от сеньоража. Рост использования мобильных денег также актуализирует проблему налогообложения экономической деятельности, поскольку операции переходят зону действия альтернативных платежных систем.

Необходимо выделить следующие риски, связанные с услугами мобильных платежей и затрагивающие макроэкономический уровень воздействия [593]:

1) системные риски, которые могут вызвать разрушение финансовой системы или «запустить» в системе негативный сценарий развития кризиса;

2) риски ликвидности, которые снижают способность банка или поставщика (агента) мобильных финансовых услуг выполнять денежные обязательства по требованию и в зависимости от величины данной организации вызвать системные сбои в макроэкономической системе страны;

3) трансграничные риски, которые позволяют распространить системный риск за пределы одного государства;

4) риски платежных систем, которые могут привести к неспособности платежных систем проводить расчеты по мере наступления срока платежа;

5) операционные риски, которые наносят ущерб способности одного из заинтересованных лиц эффективно управлять своим бизнесом, или риск, который приводит к прямым или косвенным потерям в результате неудачных внутренних процессов, людей, систем или внешних событий, в результате чего могут возникать лавинообразные последствия, затрагивающие экономику страны в целом;

6) репутационные риски, которые наносят ущерб имиджу финансовой системы.

Замещение фиатных суверенных валют частными цифровыми платежными средствами также может повлиять на денежно-кредитную политику[24] и генерировать новые риски для стабильности финансовой системы страны[25]. Ряд исследований в отношении

[24] Чтобы контролировать спрос и предложение на денежном рынке, обеспечивать его ликвидность и другие макроэкономические показатели, центральные банки используют такой инструментарий, как номинальная денежная масса или межбанковская процентная ставка. В случае невозможности напрямую регулировать спрос и предложение цифровой валюты, эффективность денежно-кредитной политики будет поставлена под сомнение [583].

[25] В настоящее время криптовалюты не имеют достаточной рыночной капитализации, чтобы оказать существенное влияние на предложение денег или иным образом повлиять на макроэкономическую политику отдельных государств [670].

денежных агрегаторов Индонезии за 2011–2018 годы показал, что рост цен на Биткойн ведет к росту инфляции, курса иностранной валюты, снижению скорости обращения денежной массы [768].

Таким образом, в финансовой сфере имплементация технологии Блокчейн связана с макроэкономическими рисками, основными из которых являются:

1) системные риски – вероятность дестабилизации финансовой системы при условии допуска к свободному обращению криптовалют на внутреннем рынке. Расширение использования криптовалюты в качестве средства оплаты товаров и услуг приведет к конкуренции с фиатной валютой, будет влиять на ее стоимость и в конечном итоге – на монетарную политику, проводимую центральным банком [683]. Многие центральные банки и финансовые регулирующие органы обеспокоены перспективой появления новых монетарных инструментов со стороны частного сектора, которые могут подорвать их способность проводить денежно-кредитную политику и поддерживать ценовую и финансовую стабильность[26] [583]. Кроме того, для государства возникает дополнительный

[26] В этой связи особое внимание уделяется планируемой эмиссии компанией Facebook в 2021 году криптовалюты Diem (ранее известной как Libra). Сеть Diem представляет собой будущую глобальную платежную сеть, которая будет работать с использованием Diem Blockchain, новой цепочки блоков, разработанной для обеспечения высокой масштабируемости, безопасности и гибкости. Согласно официальному документу, миссия проекта заключается в развитии финансовой инфраструктуры, которая «расширяет возможности миллиардов людей». Впервые проект был объявлен в июне 2019 года как единая мировая валюта, обеспеченная резервом активов. Тем не менее после тщательной проверки со стороны международных регулирующих органов Diem был пересмотрен, чтобы включить корзину одновалютных стейблкоинов с привязкой к фиатной валюте в дополнение к своей мультивалютной монете XDM. В декабре 2020 года проект был переименован с Libra в Diem. Diem, разрабатываемую Facebook, отличает сочетание сети активных пользователей, представляющих более трети населения мира, с выпуском частной цифровой валюты, непрозрачно привязанной к корзине суверенных валют. По этой причине Diem привлекает к себе пристальное внимание властей. Так, изменения в стейблкоине Diem, например в его дизайне и аспектах соответствия, вызвали озабоченность со стороны регулирующих органов. Согласно пересмотренному техническому документу, опубликованному в апреле 2020 года, наиболее значительным изменением является замена первоначальной концепции мультивалютной монеты, связанной с корзиной фиатных валют, несколькими одновалютными стейблкоинами, которые вместо этого служат элементами составной, мультивалютной монеты Diem. Поправки к Diem также подтвердили обязательства по тесному сотрудничеству и соблюдению нормативных требований, установленных центральными банками и денежно-кредитными органами. Чтобы облегчить опасения по поводу его последствий для денежного суверенитета и финансовой стабильности, Дием предложил, чтобы цифровые суверенные фиатные деньги или цифровые валюты центрального банка потенциально могли быть интегрированы в сеть Diem в будущем и в конечном итоге заменить связанные с ними стейблкоины [583].

риск неконтролируемого вывода финансовых активов из страны, без ограничений, накладываемых на движение денежных средств[27] [580]. Отмечается тенденция стирания грани между традиционными и новыми финансовыми организациями: все более распространенными становятся FinTech-кредитование в криптовалютах и банковские операции с частичным резервированием криптовалюты [670];

2) рыночные риски – высокая волатильность рынка криптовалют создает риски одномоментной потери части спекулятивных инвестиционных активов, существует угроза формирования «криптовалютного пузыря» и его негативного влияния на стабильность финансовой системы как на наднациональном, так и страновом уровнях[28] [769, 770];

3) технологические риски – недостаточная зрелость криптовалютного инструментария и инфраструктуры генерирует потенциальные

[27] В сентябре 2017 года Китай объявил о прекращении официальных обменов Биткойнов. До этого времени на долю КНР приходилось почти 90% всех операций с Биткойнами и другими криптовалютами [580]. В отчете Chainalysis утверждается, что за 2019 год из китайских цифровых кошельков в другие части мира было переведено более 50 млрд долларов криптовалюты, что указывает на возможности того, что китайские инвесторы переводят больше денег, чем разрешено, из страны [771].

[28] Схемы финансовой пирамиды (Ponzi) часто маскируются как «высокодоходные» инвестиционные программы. Комиссия по ценным бумагам и биржам США (SEC) определяет финансовую пирамиду следующим образом: Схема Понци – это инвестиционное мошенничество, которое включает в себя выплату предполагаемой прибыли существующим инвесторам из средств, внесенных новыми инвесторами. Организаторы схемы Ponzi часто привлекают новых инвесторов, обещая инвестировать средства в возможности, которые, как утверждают, приносят высокую прибыль практически без риска. Схемы Ponzi практически не имеют законных доходов или не имеют их, поэтому для продолжения работы требуется постоянный поток денег от новых инвесторов. Схемы Ponzi неизбежно рушатся, чаще всего, когда становится трудно привлекать новых инвесторов или когда большое количество инвесторов просит вернуть свои средства. Распространение смарт-контрактов создает новые возможности для мошенников, предоставляя следующие преимущества цифровых технологий: инициатор схемы Ponzi может оставаться анонимным, поскольку для создания контракта и обналичивания не требуется раскрытие личности. Поскольку смарт-контракты являются «немодифицируемыми» и «неостанавливаемыми», регуляторы не смогут прекратить выполнение схемы или обратить ее последствия, чтобы возместить расходы пострадавшим. Инвесторы могут получить ложное чувство доверия из-за того, что код смарт-контрактов является публичным и неизменным, и их исполнение автоматически обеспечивается [268]. В 2020 году криптоактивы на сумму более 4,2 млрд долларов были конфискованы китайской полицией в результате расследования финансовой пирамиды PlusToken (Chinese police have seized $4.2 billion cryptos from PlusToken Ponzi crackdown. – Режим доступа: https://www.theblockcrypto.com/post/85873/china-seize-billion-cryptos-from-plustoken-crackdown. – Дата доступа: 27.11.2020).

угрозы для стабильного развития национальных денежно-кредитных систем в случае их интеграции. Кроме того, в случае потери личного ключа доступ к криптовалютам становится безвозвратным для пользователей.

К рискам имплементации технологии Блокчейн более низкого порядка, в меньшей степени влияющих на макроэкономические условия, следует отнести:

а) энергосистемные риски – непродуктивный расход электроэнергии при майнинге создает неконтролируемый рост нагрузки для энергосистем страны дислокации криптовалютных ферм[29];

б) ПОД-ФТ-риски – дополнительный финансовый механизм отмывания денег и финансирования терроризма[30]. Проведенный США анализ киберпреступлений показал, что злоумышленники все чаще используют криптовалюту для облегчения международного финансирования терроризма, распространения оружия, уклонения от санкций и транснационального отмывания денег[31][681]. Согласно исследованию CipherTrace, банки в настоящее время не в состоянии проконтролировать подавляющее большинство подозрительных сделок [772], связанных с криптовалютами[32];

в) риски формирования рынков нелегальных товаров и услуг. Анонимность в качестве функциональной и технологической особенности криптовалют стимулирует их использование в качестве

---

[29] Согласно отчету об устойчивом развитии Биткойн, в январе 2018 года потребление энергии в Биткойнах за одну транзакцию увеличилось на 53% и составило 397 кВт·ч, что достаточно для питания 1 домохозяйства США в течение более 13 дней. В феврале 2018 года потребление электроэнергии Биткойнами возросло до 764 кВт·ч на одну уникальную транзакцию. Годовое потребление электроэнергии Биткойном увеличилось с 9,5 ТВт·ч до 50,8 ТВт·ч за последние 12 месяцев, и в феврале 2018 года Биткойн потребляет 0,23% мирового потребления электроэнергии. Точно так же увеличение было очевидно для Ethereum с 2,3 ТВт·ч до 14,5 ТВт·ч в год. По данным Кембриджского центра альтернативных финансов (Cambridge Center for Alternative Finance CCAF), Биткойн в настоящее время потребляет около 110 ТВт·ч – 0,55% мирового производства электроэнергии, что примерно эквивалентно годовому потреблению энергии в небольших странах, таких как Малайзия или Швеция [778].

[30] Исследование Foley показывает, что около четверти пользователей Биткойн и половина транзакций Биткойн связаны с незаконной деятельностью, стоимость которой достигает 72 млрд долларов США в год [779].

[31] Также для покупки и продажи контролируемых веществ, украденных и поддельных идентификационных документов и доступа к ним, устройства, контрафактные товары, вредоносное ПО и другие инструменты для взлома компьютеров, огнестрельное оружие и токсичные химические вещества.

[32] За последние два года кредитные организации смогли идентифицировать 134 500 операций, связанных с цифровыми активами, которые носили подозрительный характер. Аналитики считают, что банки не могут распознать до 90% таких транзакций.

платежного средства для транзакций в незаконном обороте отдельных товаров и услуг [773, 774]. В криптомаркетах[33] предлагаются нелегальные услуги и продукты, а также контрафактные товары[34] [775]. По одной из оценок, сумма, связанная с нелегальными онлайн-рынками (криптомаркетами), составляет около 860 млрд долларов [776]. Примером использования криптовалюты для оборота на нелегальном рынке являлся онлайн-рынок Silk Road[35]. По оценкам ФБР, в период функционирования Silk Road около 5% всей экономики Биткойн было связано с данной платформой. Согласно данным отчета компании по блокчейн-анализу Chainalysis [777], Восточная Европа проявляет «наибольшую активность на глобальном рынке даркнета по сравнению с каким-либо другим регионом». Платформа Hydra ориентирована исключительно на страны Восточной Европы и входит в число крупнейших даркнет-рынков в мире. По данным аналитиков, с июня 2019 года по июль 2020 года объем сделок на платформе Hydra составил более 1,2 млрд долларов в криптовалюте. В 2020 году объем сделок в криптовалюте на платформе Hydra достиг 1,37 млрд долларов [782]. По мнению ряда исследователей, данная платформа является крупнейшей за всю историю, в настоящее время недельный объем следок в криптовалюте достигает 125 млн долларов.

В зависимости от уровня угроз для национальной безопасности возможно дифференцировать риски использования технологии Блокчейн от минимальных до предельных. Наиболее существенными

---

[33] Криптомаркеты – это онлайновые торговые площадки, расположенные в даркнете, которые облегчают торговлю различными нелегальными товарами, в основном наркотиками. На этих торговых площадках также предлагаются различные другие товары и продукты, связанные с мошенничеством с финансами или идентификацией, огнестрельное оружие, контрафактные товары, допинговые продукты. В отличие от обычных сайтов продаж, криптомаркеты облегчают обмен в контексте, где анонимность администраторов и участников защищена благодаря комбинации функций шифрования [775].

[34] По одной из отраслевых оценок, около 1% от общего объема рыночных транзакций в 2019 году (10 млрд долларов США) были незаконными [780]. FinCEN выявил около 119 млрд долларов, связанных с подозрительной деятельностью с использованием криптовалют, которая полностью или в значительной степени осуществляется в Соединенных Штатах, что составляет около 11,9% от общей активности на рынке криптовалют. США отмечают, что злоумышленники использовали криптовалюты для содействия международному финансированию терроризма, распространению оружия, уклонению от санкций и транснациональному отмыванию денег, а также в отношении покупки и продажи контролируемых веществ, украденных и поддельных документов, удостоверяющих личность, и устройств доступа, поддельных товаров, вредоносных программ и других компьютерных хакерских инструментов, огнестрельного оружия и токсичных химикатов [781].

[35] Веб-сайт был запущен в феврале 2011 года и использовался для продажи наркотиков. В октябре 2013 года ФБР закрыло сайт.

из них являются ПОД-ФТ, преодоление санкционных ограничений на уровне государств и компаний, опосредованное стимулирование формирования рынка краденых цифровых активов, осуществление мошеннических операций[36], расширение использования программ вымогателей. Следует также выделить ряд рисков, генерируемых инструментарием DeFi, основными из которых являются валютный и платформенный.

Важно отметить, что с учетом наращивания технологического потенциала регуляторов киберпреступники расширяют использование таких цифровых решений, как [673]:

а) технологии смешивания[37] (миксера) – сервисы, предназначенные для скрытия взаимосвязи между адресами в последовательных транзакциях [783];

б) альткойны с внутренними конструкциями, повышающими конфиденциальность. К данным альткойнам относятся Zerocoin, Zerocash, Zcash[38] и Dash; дизайн CryptoNote[39], включая Monero, Bytecoin и DigitalNote.

---

[36] Мошенничество снова стало крупнейшей формой преступлений, связанных с криптовалютой: в 2021 году по всему миру было похищено в криптовалюте на сумму более 7,7 млрд долларов, рост на 81% по сравнению с 2020 годом. Только благодаря российской финансовой пирамиде Finiko произошло хищение более 1,1 млрд долларов.

[37] Услуги смешивания направлены на решение проблем с отслеживанием криптовалют путем объединения нерелевантных транзакций. Два типичных типа смешивания – это своппинг и CoinJoin. Сервис микширования на основе свопинга принимает депозиты от пользователей на один из адресов в адресном пуле и снимает их с другого. В результате нивелируется связь между адресами ввода и вывода. Сервисы смешивания с использованием свопинга включают BitcoinFog, BitLaundry и Helix. Механизм CoinJoin позволяет объединить две или более отдельных транзакций в одну транзакцию CoinJoin, которая имеет такое же присутствие в Блокчейн, как обычная транзакция с несколькими входами и несколькими выходами. Следовательно, связь между реальными парами ввода-вывода неясна. Сервисы на основе CoinJoin включают JoinMarket, CoinShuffle и SharedCoin Blockchain.info (обслуживание прекращено).

[38] Zcash позволяет пользователям хранить и осуществлять транзакции ZEC, то есть криптовалюту Zcash, с двумя типами адресов (прозрачными и защищенными). «Прозрачные» адреса передают значения на другие адреса, по сути, так же, как Биткойн, в то время как «защищенные» адреса совершают транзакции в «защищенных пулах». В частности, при внесении депозита в пул получатель указывается с использованием экранированных адресов, то есть Z-адреса, который скрывает получателя, но по-прежнему раскрывает отправителя, а выход из пула скрывает отправителя, но раскрывает получателя. Криптографическая основа защищенного пула – это практические доказательства с нулевым разглашением, называемые zfc-SNARK. С точки зрения моделей данных транзакции Zcash напоминают схему пула смешивания подкачки.

[39] Криптовалюты, подобные CryptoNote, такие как Monero, используют другую технологию – кольцевую подпись, чтобы усложнить записи транзакций, не вызывая больших вычислительных затрат. Транзакция Monero позволяет объединить несколько выходов из предыдущих транзакций в качестве входов, но только некоторые из входов могут быть «обманчивыми», поскольку их значения никогда не передаются в выход.

Отмечается тенденция стирания грани между традиционными и новыми финансовыми организациями: все более распространенными становятся FinTech-кредитование в криптовалютах и банковские операции с частичным резервированием криптовалюты [670].

Исследования МВФ [784] показывают, что усиление роли FinTech расширяет доступ населения к кредитам, что в сочетании с низким качеством банковского надзора за FinTech-организациями ставит под угрозу макрофинансовую стабильность в стране [785].

В отчете Совета по финансовой стабильности (FSB) были определены в том числе следующие риски, связанные с FinTech [738, 786, 787].

1. Рост кредитования онлайн-платформ в условиях слабых стандартов кредитования повышает вероятность того, что широко распространенные дефолты могут спровоцировать кризис.

2. Секьюритизация кредитов, предоставляемых кредиторами на рынке FinTech, может быть особенно рискованной, поскольку потенциальные дефолты заемщиков приведут к снижению кредитоспособности системы и снижению цен на эти активы.

3. Потенциальный пузырь в государственных или частных акциях FinTech-компаний может привести к негативным последствиям для финансовой системы.

Как отмечает Скардови [559], стабильность глобальной финансовой системы все в большей степени зависит от растущего цифрового характера рисков:

1) вводящая в заблуждение информация о состоянии кредитного рынка может привести к невозможности сбалансировать предложение на кредитование на платформах P2P и реальной способности заемщиков погасить свой долг[40];

2) центральным банкам становится сложнее контролировать показатели кредитования, поскольку кредитная активность FinTech-организаций частично зависит от базовой процентной ставки экономики, не регулируется инструментарием минимальных резервных требований, определяемых регулятором в отношении банков;

---

[40] Теоретически взаимодействие спроса и предложения на кредитование на платформах P2P должно иметь тенденцию приспосабливаться к реальной способности заемщиков погасить свой долг (как мера с помощью более информированных и более интеллектуальных инструментов оценки поведения, основанных на ML/AI и использующих структурированные и неструктурированные данные), с учетом отдачи, которую они могут получить от своих инвестиционных проектов или моделей потребления, что соответствует их экономическому жизненному циклу.

3) FinTech-организациям постепенно переходит ответственность за преобразование сроков погашения долгов, что может привести к нехватке ликвидности и рыночным крахам, если большинство выданных FinTech-ссуд станут невозвратными и потребуется реструктуризация и списание долгов, особенно с учетом внезапных изменений процентной ставки экономики (если инфляция снижается, долги по фиксированным ставкам становятся все менее устойчивыми);

4) увеличение скорости использования капитала, обусловленное финансовыми инновациями, может стать важным компонентом цифровых рисков. Высокочастотная торговля, пулы и использование альтернативных торговых площадок становятся управляемыми сверхскоростными алгоритмами, генерируемыми искусственным интеллектом, которые могут потенциально разрушить рынки в случае цифровых ошибок в используемых алгоритмах.

Отдельным фактором развития FinTech становится его подверженность монополизации, поскольку цифровые данные становятся самым ценным активом, способствующим росту прибыльности в различных секторах и цепочках создания стоимости[41]. Выход крупных технологических компаний на рынок финансовых услуг делает этот рынок эффективнее, но в то же время создает риски для финансовой стабильности и конкуренции. Крупные технологические компании на рынке финансовых услуг предлагают различного рода FinTech-инструменты, включая банковские, платежные и краудфандинговые сервисы, кредиты, страховки, возможности для управления активами. При этом глобальные игроки благодаря инновационности используемых крупных бизнес-моделей, технологий и сетевых эффектов, которые усиливаются недостаточным регулированием и возможностью регуляторного арбитража, имеют возможность монополизации кредитного рынка, отводя традиционным банковским институтам лишь роль источника фондирования. Кроме того, FinTech-компании имеют возможность манипулировать поведением своих пользователей, создавать собственные платежные

[41] Alphabet (Google), Apple, Microsoft, Facebook, Amazon контролируют большое количество данных, и экономия от масштаба вызывает беспокойство со стороны регуляторов, ответственных за поддержание конкуренции, поскольку их размер и охват усугубляются всевозможными сетевыми эффектами. Конкурентное преимущество обусловлено владением большими данными, которое предоставляет возможность (или угрозу) для создания непреодолимого конкурентного «разрыва», используемого немногими владельцами мегаданных «разделяй и властвуй» (разделяя конкурентов и остальную часть рынка, чтобы в конечном итоге доминировать над обоими).

системы с эмиссией стейблкойнов, предназначенных для эксклюзивного использования в этих системах (DeFi), что обеспечивает дополнительные их конкурентные преимущества на рынке. Профессор Принстонского университета Бруннермайер [613] убежден, что объективные рыночные преимущества FinTech приведут к еще большей концентрации рыночной власти у нескольких компаний и фрагментации денежно-кредитной системы, а также эрозии монетарного суверенитета стран. Вероятность такого развития FinTech поддерживает и управляющий BIS Карстенс, который отмечает, что технокомпании крайне быстро переходят из категории «слишком мелких, чтобы о них думать» (too small to care), в категорию «слишком больших, чтобы их игнорировать» (too big to ignore), а затем и «слишком больших, чтобы допустить их банкротство» (too big to fail).

Как отмечает ряд исследователей [788], внедрение IT-технологий в производственные процессы и связанная с ними цифровизация и виртуализация определяют три разнонаправленные тенденции, каждая из которых может стать как доминирующей, так и внешней тенденцией, в зависимости от проводимой в стране экономической политики.

Первая тенденция – высвобождение рабочей силы, поскольку потребность экономики в физическом труде уменьшается. Преобладание этой тенденции увеличивает безработицу в экономике, приводит к снижению спроса на национальном рынке и в конечном итоге может вызвать экономическую деградацию[42]. В исследовании, проведенном McKinsey Global Institute [335], отмечено, что во многих отраслях промышленности к 2030 году благодаря появлению новых технологий и автоматизации вероятно сокращение 73 млн рабочих мест [740]. Исследование перспективы автоматизации с помощью цифровых технологий, робототехники и AI, проведенное Фреем и Осборном [789, 790] показало, что 47% рабочих мест в США рискуют стать избыточными[43]. Цифровизация затронет рабочие места во многих отраслях и секторах, включая промышленное производство, логистику, образование, госуправление, здравоохранение [321].

[42] Пик негативного влияния компьютеризации на уровень занятости населения прогнозируется в 2020–2030 годах. Министерство труда России оценивает количество людей, которые потеряют работу в этот период, от 30 до 40% национальной рабочей силы [788].

[43] В 2000 году Goldman Sachs имела в штате шестьсот трейдеров, а благодаря внедрению AI в 2017 году корпорация смогла сократить число трейдеров-людей до двух [793].

Вторая тенденция связана с повышением производительности труда. Рост производительности труда в масштабах национальной экономики ведет к ужесточению конкуренции, снижению затрат и цен на инновационную продукцию, а также обеспечивает укрепление конкурентных позиций национального производителя в мировой экономике. Национальная рабочая сила востребована как ресурс для мирового производства, что увеличивает спрос на нее, ведет к повышению заработной платы и покупательной способности занятых. По мнению WEF [791], синергия технологий и человека дает устойчивый прирост производительности, в то время как автоматизация ради сокращения рабочей силы дает только временные улучшения. Ряд исследований подчеркивают, что инвестиции в цифровые технологии (роботы, 3D-печать, IoT), которые подпитывают текущую промышленную революцию, положительно влияют на занятость высококвалифицированных работников и отрицательно влияют на занятость низкоквалифицированных работников [789]. Согласно докладу Комитета по науке и технике Палаты общин Великобритании (2016)[44], недостаток цифровых навыков рабочей силы представляет собой проблему государственного уровня[45] [740, 792]. В сочетании с сокращением рабочих мест для низкоквалифицированных работников и особенностями отдельных социальных групп, не обладающих технологическими навыками (например, пожилыми людьми) неравенство среди населения, как прогнозируется, будет увеличиваться. В отчете Всемирного экономическогор форума «Будущее рабочих мест» говорится, что автоматизация может привести к сокращению 85 млн рабочих мест всего за пять лет [791]. Ожидается, что как в развитых, так и в странах с формирующейся экономикой быстрый переход к удаленной работе приведет к долгосрочному повышению производительности, но при этом рискует создать новые разрывы между специалистами и теми, кто занят в производственных секторах и не может работать удаленно, либо могут не иметь цифровых навыков и инструментов для поиска другой работы в таких областях, как производство, розничная торговля и некоторые области здравоохранения. Расширение разрыва в цифровой грамотности создает риск создания «цифрового низшего класса».

---

[44] House of Commons Science and Technology Committee (STC).

[45] Комитет определил данную проблему как «кризис цифровых навыков» в Великобритании. Основной движущей силой кризиса является сложность подбора надлежащим образом подготовленного персонала. По оценкам C. Frey, M. Osborne [790], 30% рабочих мест в Великобритании подвергается риску автоматизации в течение следующих 10–20 лет.

Третья тенденция связана с изменением структуры экономики и рынка труда. Увеличивается доля занятых высококвалифицированных кадров, наблюдается рост инновационных отраслей экономики. С развитием интеллектуальных систем все большее число услуг будет доступно через интеллектуальные устройства и Интернет [528]. К 2025 году в результате разделения труда между людьми, машинами и алгоритмами может появиться 97 млн новых рабочих мест [791]. Согласно ряду исследовапний [794, 795], компании будут стремиться использовать преимущества AI по следующим направлениям: а) увеличивая разрыв в заработной плате между квалифицированным и неквалифицированным трудом, так как последний предположительно более заменим AI, чем первый; б) автоматизируя контрольные задачи; в) поощряя самозанятость. По данным отчета McKinsey, COVID-19 ускорил внедрение автоматизации и AI, поскольку предприятия стремятся контролировать свои затраты и повышать эффективность за счет сокращения доли занятых, выполняющих рутинные задачи. Компании достигают поставленной задачи двумя способами: внедрением технологий автоматизации и изменением рабочих процессов[46][181]. AI, таким образом, становится важным инструментом, который будет замещать такие направления деятельности, как бухгалтерский и складской учет, логистика, внутренний и внешний аудит, административный и торговый функционал, клиентское обслуживание, банковская сфера, страховое обслуживание, юриспруденция и пр. Востребованность на рынке приобретут специальности на стыке IT-технологий (AI, ML, BDA), аналитики, теории и практики функционирования современных бизнес-моделей. В разрезе профессий до 2030 года под влиянием ускоренной цифровизации и внедрения новых технологий после пандемии COVID прогнозируется положительный сдвиг в занятости в таких профессиях, как врачи и медсестры, научные и технические специалисты, менеджеры, а также креативные профессии. Сократится спрос на занятых в коммунальном хозяйстве, строителей, офисных работников, ресторанном бизнесе, сельском хозяйстве [181].

С учетом изложенного, представляется наиболее вероятной определенная конвергенция трех тенденций, которая будет проявляться в структурной трансформации экономик развитых государств,

[46] В глобальном опросе 800 руководителей в июле 2020 года 2/3 заявили, что они активизируют свою деятельность и вложения в автоматизацию и искусственный интеллект – частично или значительно.

росте сектора ИКТ и цифровых сегментов традиционных отраслей, требующих высококвалифицированных специалистов. При этом будет отмечаться снижение занятости в отраслях первичного сектора экономики и перетекание трудовых ресурсов в сектор услуг, который в наименьшей мере будет в среднесрочной перспективе подвержен тотальной цифровизации. В данном контексте задачей государства является обеспечение плавного перетока трудовых ресурсов из менее производительных секторов в более производительные. Лица, которые по объективным (субъективным) причинам неспособны освоить цифровые навыки, станут фокусной группой для государственной поддержки. Одним из механизмов социального обеспечения для данной группы граждан может служить базовый доход. Обеспечение плавного перехода к цифровым технологиям и снижение рисков для социальной стабильности из-за цифрового разрыва потребует со стороны государства системного управления инновациями, не ограничивая их, – например, настаивая на безопасности и конфиденциальности при разработке новых технологий и цифровых услуг.

В Республике Беларусь как на уровне макроэкономики, так и социальной среды важнейшее влияние цифровизации будет проявляться в расширении «цифрового разрыва»[47] как между различными категориями граждан и внутри отраслей (сегментов) экономики страны, обостряя цифровое неравенство, положительно влияя на занятость высококвалифицированных работников и отрицательно – на занятость низкоквалифицированных работников. Экстраполяция выявленных тенденций и динамки цифровизации передовых стран Европы, Азии и США [181] на рынок труда Республики Беларусь позволяет прогнозировать положительный сдвиг занятости в таких профессиях, как медицинские работники, научные и технические специалисты, персонал креативных отраслей. Вместе с тем также высока вероятность сокращения спроса на рынке труда в коммунальном хозяйстве, строительстве, образовании, офисного и торгового персонала, складской логистике, сельском хозяйстве. В случае, если будут доминировать характеристики трансформации рынка труда, свойственные развивающимся странам (Индии и КНР), сокращение затронет, главным образом, сектор сельского хозяйства Беларуси в объеме около 8%, или около 30 тыс. человек

[47] Разрыв в цифровом образовании, в условиях доступа к цифровым услугам и продуктам и, как следствие – разрыв в уровне благосостояния.

(отталкиваясь от статистических показателей 2019 года). Кроме того, в зоне риска находятся также рабочие места в сфере администрирования, общественного питания, продаж и складской логистики. Ускорение и углубление цифровизации повысит требования к занятым во многих отраслях и секторах, включая промышленное производство, образование, госуправление, здравоохранение, стимулируя рост безработицы среди низкоквалифицированной рабочей силы.

На глобальном экономическом форуме были резюмированы разнонаправленные эффекты цифровизации экономики [796]. Среди актуальных рисков внедрения цифровых инноваций в краткосрочной перспективе (0–2 лет) – недостаточная кибербезопасность[48] и цифровое неравенство[49]; в среднесрочной перспективе (3–5 лет) – взлом IT-инфраструктуры[50], недостаточная кибербезопасность и ошибки в управлении технологиями[51]; долгосрочные риски (5–10 лет) – неблагоприятные технологические достижения[52]. В авторитарных государствах существует угроза того, что правительства попытаются захватить главные платформы и поставщиков услуг, тем самым консолидирует свою власть по ограничению доступа в Интернет, цензуре информации и сокращению коммуникаций[53]. Пути к будущим экономическим и социальным выгодам в этих условиях будут под угрозой.

---

[48] Инфраструктура и (или) меры кибербезопасности бизнеса, правительства и домашних хозяйств опережают или становятся устаревшими из-за все более изощренных и частых киберпреступлений, что приводит к экономическим сбоям, финансовым потерям, геополитической напряженности и (или) социальной нестабильности.

[49] Фрагментированный и (или) неравный доступ к важнейшим цифровым сетям и технологиям между странами и внутри стран в результате неравных инвестиционных возможностей, отсутствия необходимых навыков у рабочей силы, недостаточной покупательной способности, государственных ограничений и (или) культурных различий.

[50] Ухудшение работы или остановка критически важной физической и цифровой инфраструктуры или услуг в результате системной зависимости от киберсетей и (или) технологий: систем с интенсивным использованием AI, Интернета, портативных устройств, коммунальных служб, спутников и т. д.

[51] Отсутствие общепринятых структур, институтов или правил для использования критически важных цифровых сетей и технологий в результате того, что разные государства или группы государств принимают несовместимую цифровую инфраструктуру, протоколы и (или) стандарты.

[52] Преднамеренные или непреднамеренные негативные последствия технического прогресса для людей, бизнеса, экосистем и (или) экономики: AI, интерфейсы мозг-компьютер, биотехнологии, геоинженерия, квантовые вычисления и т. д.

[53] Возможным решением данной угрозы может быть развертывание спутниковых группировок для предоставления бесплатного доступа в Интернет.

Агрегируя данные проведенного анализа, можно выделить следующие макроэкономические угрозы цифровизации в отношении различных аспектов экономического развития страны (табл. 2.2).

Таблица 2.2

Риски и угрозы цифровизации в разрезе макроэкономического развития (разработано автором)

Макроэкономические показатели	Направление влияния рисков и угроз	
	препятствующее росту	стимулирующее рост
Инфляция	–	Расширение кредитно-финансовой деятельности FinTech, в особенности с использованием криптовалюты, может привести к перетоку фиатных денежных активов в криптоактивы, стимулируя инфляцию
Национальный доход	Рост темпов автоматизации и цифровизации приведет к цифровому разрыву и высвобождению рабочей силы и падению доходов низкоквалицифированной рабочей силы; развитие FinTech-индустрии будет способствовать снижению процентов по кредитам	–
ВВП	Сокращение показателей национального дохода может оказать негативное влияние на рост ВВП	–
Международная торговля	Несогласованное на международном уровне внедрение концепции CBDC приведет к негативному влиянию на международные платежи, препятствуя росту международной торговли	–
Международные финансы	Расширение использования CBDC, укрепление доверия и стабилизация криптовалютных рынков приведет к трансформации текущей мировой финансовой системы, возможной ее дестабилизации	–

Окончание табл. 2.2

Макроэкономические показатели	Направление влияния рисков и угроз	
	препятствующее росту	стимулирующее рост
Безработица	–	Автоматизация и цифровизация все большего количества производственных и бизнес-процессов, внедрение FinTech-инноваций, E-Government будут стимулировать расширение цифрового разрыва населения, росту безработицы низкоквалифицированной рабочей силы
Сбережения и инвестиции	Внедрение технологий CBDC сокращает кредитные ресурсы коммерческих банков за счет «отмены» традиционных депозитных механизмов	Аккумулирование значительных финансовых ресурсов глобальными ИКТ компаниями (их капитализация) приведет к росту инвестиций в цифровой сфере

Заключение

Таким образом, следует отметить, что цифровизация создает определенные риски и угрозы на уровне макроэкономики, затрагивая такие ее элементы, как инфляция, национальный доход, ВВП, международная торговля, международные финансы и безработица. При этом наиболее уязвимыми элементами макроэкономики для цифровых рисков являются международные финансы и безработица. Технологии AI/ML, IoT, BDA, концепции CBDC, FinTech позволяют автоматизировать бизнес-процессы, сократить количество рутинных операций, меняя, тем самым рынок труда, генерируя новые вызовы в отношении государственной социальной политики.

В Республике Беларусь можно с высокой степенью уверенности прогнозировать сокращение спроса на персонал в коммунальном хозяйстве, строительстве, образовании, офисном и торговом администрировании, складской логистике.

Концепции CBDC, FinTech, формируя новые цифровые рынки мобильных денег и криптовалют, создают потенциальные риски для стабильности функционирования финансовой системы не только на национальном, но и международном уровне. В этой связи актуализируется проблематика качества банковского надзора,

цифровых компетенций регулятора. Высокая динамика имплементации цифровых концептов, рост скорости использования капитала вызывают необходимость трансформации подходов и инструментария кредитно-денежной политики центральных банков.

Высокочастотная торговля, инвестиционные пулы, управляемые сверхскоростными алгоритмами, генерируемые AI для проведения транзакций на альтернативных (нерегулируемых) торговых площадках, создают потенциал разрушения рынков в случае цифровых ошибок. Дополнительным фактором нарастающего цифрового риска является рост киберпреступности, использующей криптовалютный инструментарий для противоправной деятельности.

Концепция E-Government, формирующая новую цифровую инфраструктуру взаимодействия экономических агентов и государства, создает потенциал для роста рисков и угроз в контексте как безопасности, так и устойчивости системы госуправления. Как показал анализ eGMM, наибольший многосторонний потенциальный ущерб для различных систем государственного управления связан с имплементацией E-Government 4.0, как самой комплексной версией концепта. Данный факт предопределяет необходимость детальной системной проработки государством данного концепта в разрезе рисков и угроз на технологическом, организационном, правовом и экономическом уровнях с целью нивелирования (минимизации) урона экономической, социальной средам и системе госуправления.

2.3. Угрозы и риски цифровой экономики в секторальном разрезе

Цифровизация экономики ведет к формированию не только макроэкономических рисков, но и рисков, затрагивающих определенные сектора, отрасли, а также имеющие потенциал для мультиотраслевого (мультисекторального) распространения. Кроме того, цифровые технологии, включая Big Data, AI/ML позволяют отдельным компаниям на секторальном уровне агрегировать большие массивы персональных данных клиентов для целей ценовой дискриминации[54].

Следует отметить, что цифровизация отраслей современной экономики в направлении их адаптации соответствующих концептов

[54] В условиях олигополии это приводит к ослаблению ценовой конкуренции.

«Новой экономики 2.0» предполагает внедрение комплекса информационных систем, включающих общие технологические компоненты (IoT, BDA, AI, Blockchain, Cloud) и бизнес-операционные (производственные) системы (табл. 2.3).

Таблица 2.3

Цифровые технологические решения в рамках концепций «Новой экономики 2.0» (разработано автором)

Промышленность (Industry 4.0)	IoT, BDA, AI, Блокчейн, Cloud	PDM, MES ERP, CAD, CAE, CAPP, SSM, CRM, PLC, CALS, SCADA, CAM, KM, 3D, TQM, BPM, Rob
Финансовый сектор (FinTech)	BDA, Блокчелйн, AI, Cloud	ERP, RPA, SSM, CRM, KM
Энергетика (Smart Grid)	BDA, Блокчейн, IoT, Cloud	ERP, SSM, CRM, SCADA, CAM, KM, BPM
Сельское хозяйство (Agriculture 4.0)	IoT, Cloud	PLC, CALS, AITS
Строительство (Smart Construction)	IoT, Cloud	BIM, KM, BPM, Rob
Транспорт и логистика (Smart Supply Chain)	BDA, IoT, Cloud	ERP, SSM, CRM, KM, BPM
Торговля (E-Commerce)	BDA, Cloud	ERP, SSM, CRM, PLC, CALS, KM

Примечание. 3D – аддитивные технологии и системы; AITS – система идентификации, регистрации, прослеживаемости животных и продукции животного происхождения; BIM (Building Information Modeling) – системы информационного моделирования в области промышленного и гражданского строительства; BPM (Business Perfomance Managment) – процессное управление организацией; CAD, CAE (ComputerAided Design; Computer-Aided Engineering) – системы цифрового проектирования и моделирования [797]; CAPP (Computer-Aided Process Planning) – системы планирования производства; ERP (Enterprise Resource Planning) – цифровая система планирования ресурсов предприятия [798]; KM (Knowledge Management) – управление знаниями и навыками на различных уровнях управления; MES (Manufacturing Execution System) – цифровая система управления производственными процессами; PDM (Product Data Management) – системы управления инженерными данными; PLC, CALS (Product Life Cycle, Continuous Acquisitionand Lifecycle Support) – системы управления жизненным циклом промышленного продукта; SCADA, CAM (Supervisory Control And Data Acquisition, Computer-Aided Manufacturing) – системы автоматизации цеховых процессов; SSM, CRM – системы продажи и управления сервисом; SCM (Supply Chain Management) – системы управления цепочками поставок; TQM (Total Quality Managment) – модули общего управления качеством; Rob – робототехнические (роботизированные) системы и автоматы.

Согласно эмпирическим оценкам рисков и угроз по основным системам управления и интеллектуализации, наиболее уязвимыми системами с точки зрения киберугроз, риски взлома которых потенциально могут нанести максимальный урон деятельности предприятий, являются PDM, SCADA, CAM, MES, BPM, системы ИИ, IoT и роботизированные устройства конвейера.

Ключевыми блоками рисков имплементации технологических решений IoT, Cloud, AI, BDA, Блокчейн, как показано в табл. 2.4, в экономическую, социальную, общественную системы являются кибербезопасность систем, конфиденциальность данных, отсутствие общих стандартов и совместимость.

Таблица 2.4

Уязвимости современных технологий, интегрированных в цифровые концепты

(разработано автором на основе [203, 217, 219, 221, 242, 799-807])

Цифровые риски и угрозы	Цифровые технологии				
	IoT	Cloud	AI	Big Data	Блокчейн
Кибербезопасность[55]	DDos[56]	Потеря управления над отдельными блоками цифровых данных, передаваемых под контроль облачному провайдеру	Взлом и нарушения работы алгоритмов	Взлом и несанкционированный доступ к коммерчески чувствительной информации	Риски на уровне транзакций

[55] По мнению Минобороны США, в настоящее время у производителей IoT оборудования практически отсутствует стимул для разработки функций безопасности в программном обеспечении своих продуктов [217].

[56] В ботнете IoT различные скомпрометированные интеллектуальные объекты loT, такие как камеры, датчики и носимые устройства, зараженные вредоносным ПО, позволяют злоумышленнику контролировать интеллектуальные объекты IoT для выполнения действий, как в традиционном ботнете. Основное различие между традиционным ботнетом и бот-сетями IoT заключается в том, что в последнем случае зараженные устройства IoT продолжают распространять свое вредоносное ПО на многие другие устройства. Ботнет loT имеет больший масштаб по сравнению с традиционным ботнетом. В 2016 году в США осуществлена DDOS-атака под названием «Mirai», в результате которой было заражено большое количество устройств IIoT, включая видеорегистраторы и камеры видеонаблюдения. Эти скомпрометированные устройства затем использовались для инициирования DDOS-атак против поставщика услуг DNS «DYN» путем загрузки массива трафика данных в формате поисковых запросов DNS [808].

Продолжение табл. 2.4

Цифровые риски и угрозы	Цифровые технологии				
	IoT	Cloud	AI	Big Data	Блокчейн
Кибербезопасность	МС[57]	Уязвимость интерфейса управления	Принятие ошибочных решений системами в рамках FinTech, высокие потенциальные финансовые издержки	Взлом и несанкционированный доступ к коммерчески чувствительной информации	Риски на уровне транзакций
	SC	Безопасность ПО, инфраструктуры, хранения, сети, среды облачных вычислений			
	Шпионаж				
Конфиденциальность	Отсутствие строгих правил в отношении сбора и использования данных	Генерируются риски в области защиты данных для клиентов и поставщиков облачных услуг		Получение несанкционированного доступа к персональным данным	Использование общедоступных систем Блокчейн не дает возможности полного контроля конфиденциальности
	Отсутствие многофакторных моделей, обеспечивающих прозрачность и выполнение	Неполное удаление данных		Получение несанкционированного доступа к коммерческой информации	

[57] При наличии уязвимостей программного обеспечения злоумышленник может получить действительный ключ сеанса или каким-либо образом перехватить сетевой трафик. Таким образом, злоумышленник может контролировать всю систему. Проведенный анализ трафика даркнета в мае 2018 года выявил цифровые данные с более 129 тыс. уникальных устройств IoT, распределенных в 199 странах (основными были Мексика (14%), Бразилия (12%), Китай (9%), Индонезия (5%), Россия (4%), США (4%), и Вьетнам (4%)), размещенных в 43 различных секторах. Наиболее затронутыми секторами стали провайдеры Интернет-услуг, телекоммуникации [803].

Продолжение табл. 2.4

Цифровые риски и угрозы	Цифровые технологии				
	IoT	Cloud	AI	Big Data	Блокчейн
Конфиденциальность	Ограниченные ресурсы для создания IoT-устройств, разработанных в соответствии с реализацией принципов конфиденциальности	Анонимность данных имеет такие уязвимости, как скрытая идентификация, пробелы в процедурах повторной идентификации или деанонимизации		Получение несанкционированного доступа к государственным секретам	
	Отсутствие защиты данных, собираемых устройствами IoT				
Стандартизация	Отсутствие единых стандартов (различные стандарты разработаны IEEE, IETF, ITU, ISO, IEC, 3GPP	Недостаточное количество инструментов, процедур, стандартных форматов данных или интерфейсов служб, которые могли бы гарантировать переносимость данных, приложений и услуг. Это может затруднить для клиента переход от одного поставщика к другому			Отсутствие общепризнанной стандартизации

Окончание табл. 2.4

Цифровые риски и угрозы	Цифровые технологии				
	IoT	Cloud	AI	Big Data	Блокчейн
Совместимость	Отсутствие стандартов функциональной совместимости				
	Отсутствие стандартных конфигураций для взаимодействия с большим количеством IoT-устройств				
Правовое регулирование	Отсутствие защиты информации в нормативных актах в сфере трансграничного обмена данными		Отсутствие защиты потребителей от использования манипулятивных AI технологий	Отстутствие защиты конкурентной среды от попыток монополизации рынков за счет обладания эксклюзивной информацией Big Data	Распределенная природа Блокчейн позволяет системе функционировать одновременно в нескольких юрисдикциях
	Отсутствие законодательства о дискриминационном использовании данных IoT		Отсутствие защиты работников и потребителей от внедрения AI со стороны корпораций		
	Отсутствие законодательства об использовании данных для борьбы с преступностью				

Примечание. DDos – атаки систем IoT с помощью сети ботов, MC – вредоносный контроль над незащищенными элементами системы IoT; SC – сканирование системы IoT с помощью специального оборудования с целью кражи цифровых данных; шпионаж – использование уязвимости системы для проникновения в систему и кражи информаци

Важно отметить, что системы IoT [185] связаны при наличии реальных активов, объединенных в сети и контролируемых через Интернет, не только с экономическими или социальными рисками и угрозами, но и физической безопасностью граждан. Таким образом, представляется возможным рассматривать данные технологии в разрезе киберфизической безопасности. Кроме того, системы IoT [302] являются гетерогенными по своей природе, что увеличивает сложность механизмов безопасности и конфиденциальности.

Для таких секторов, как промышленность, сельское хозяйство, энергетика (включая ядерную энергетику), логистика (включая транспортную инфраструктуру), городское управление, выделяют риски, связанные с внедрением технологий IoT, включая кибербезопасность, обеспечение конфиденциальности данных, отсутствие нормативных стандартов и, соответственно, несовместимость гетерогенных систем, лакуны в законодательном регулировании. Системы IoT связаны не только с экономическими или социальными рисками и угрозами, но и физической безопасностью граждан, генерируют, таким образом, киберфизические угрозы.

Кроме того, они в настоящее время обрабатываются централизованными облачными системами управления данными, что увеличивает их уязвимость, актуализируя проблематику целостности, конфиденциальности и доступности информационных защиты данных от несанкционированного доступа, изменения или удаления [807]. Существует риск безопасности прикладных приложений и промышленных облачных платформ в условиях ограниченности их полноценной изоляции от внешних сетей[58]. Внедрение облачных технологий в таких секторах, как банковский, телекоммуникации, производственные предприятия, формирует следующий корпус угроз и рисков: безопасность используемого программного обеспечения; надежность инфраструктуры; гарантирование безопасности хранения цифровых данных; сетевая безопасность; гарантия анонимности данных; обеспечение целостности, конфиденциальности и доступности информации.

В целом следует отметить, что расширение открытого, взаимосвязанного и интеллектуального развития в производственной, сельскохозяйственной, транспортной, энергетической сферах, торговле

[58] В 2020 году производитель электроники Garmin стал жертвой вируса-вымогателя WastedLocker, который зашифровал внутреннюю сеть компании и некоторые производственные системы. В результате кибератаки были заблокированы функционильные операции внутренних сервисов, колл-центра, сайта и промышленного производства.

и коммунальном хозяйстве сталкивается с серьезными проблемами безопасности [211]. Технологические инновации способствуют интеграции Интернета и традиционных отраслей, подключению большого количества производственного оборудования и систем управления к сети. Сложность оцифрованных производственных (торговых, транспортных) сред фактически определяется наличием двух взаимосвязанных основных сетей: информационной и производственной (торговой, транспортной) [809]. Результирующие взаимосвязанности в оцифрованных средах создает большие уязвимости для атаки и больше возможностей для их распространения.

Кибератака может распространяться по всей информационной сети и наносить значительный ущерб как информационной, так и производственной сети[59]. Таким образом, ущерб, вызванный кибератакой, не только снижает функциональность самого атакованного сетевого узла, но и может распространяться как в информационных, так и в производственных сетях из-за их взаимосвязанности. Кроме того, промышленные системы управления (ICS) традиционно функционировали в изолированных средах. С развитием информационных и коммуникационных технологий и функциональных требований все больше ICS переводится в общедоступную сеть для обеспечения удаленного контроля и надзора за инфраструктурами [811]. Данный фактор увеличивает вероятность внешнего злонамеренного проникновения во внутренние системы управления предприятиями.

Тенденция внедрения интеллектуальных систем в энергетические системы (как на уровне интеллектуальных диспетчерских систем, так и систем управления) актуализировала проблематику рисков цифровизации для стабильного функционирования данного направления не только в секторальном разрезе, но и национальных экономик в целом. Smart Grid характеризуется быстрым двусторонним потоком информации между составными элементами сети, блоками генерации, передачи, распределения и потребителями [812][60]. Распределенные гетерогенные энергогенерирующие

[59] По данным отраслевого регулятора Великобритании Make UK, в 2018 году 24% британских производителей понесли финансовые или иные убытки в результате кибератак [810].

[60] Например, «умный» счетчик может передавать информацию с сайта клиента на компьютер поставщика услуг. Если этот поток информации должен осуществляться по беспроводной сети или через общедоступные сети, каналы данных, возможно, должны быть защищены. Этот массивный поток данных может представлять серьезные проблемы кибербезопасности.

мощности, гибкие нагрузки и внешние природные и антропогенные факторы влияют на безопасность и стабильную работу электрических сетей [21]. Важн о отметить, что концепция Smart Grid предполагает цифровизацию основных четырех компонентов энергосистемы: энергогенирирующих мощностей, энергопередачи, распределения и конечного потребления, каждый из которых является уязвимым для разного вида внешних атак. Проведенное в 2016 году исследование [813] о зарегистрированных атаках в США показало, что энергетическая инфраструктура являлась целью таких атак в 54% случаев [814].

Важно отметить, что электроэнергетика является составной частью критической национальной инфраструктуры, которая определяет стабильность функционирования жизненно важных сфер в контексте, в том числе экономической безопасности государства. Любая система может стать критической, когда уязвимости становятся угрозами, вызывающими различные виды разрушительного воздействия на социальные системы, энергетику, безопасность, здоровье населения и важные элементы общества[61]. Отказ инфраструктуры

[61] В 2013 году была взломана плотина Боумен-авеню в г. Нью-Йорке (США) и хакерам удалось получить контроль над шлюзами. Исследования показали, что они могли легко изменить параметры, связанные с потоком воды или даже изменить количество химических веществ, используемых при обработке воды, до катастрофического эффекта, что привело бы к разрушительным последствиям. В 2016 году хакеры проникли в систему управления водоканала Kemuri Water Company (США) и изменили уровни химикатов, используемых для обработки водопроводной воды, манипулируя клапанами, контролирующими поток химикатов. В 2016 году при целенаправленной DDoS-атаке было отключено тепло и горячая вода в двух жилых домах Финляндии в середине финской зимы [814]. В 2018 году, по данным службы безопасности Украины, была осуществлена кибер-атака на станцию очистки воды ООО «Аульский хлорный завод» (обслуживает население в Украине, Молдове и Беларуси), организованная иностранным государством. При атаке использовалось вредоносное программное обеспечение VPNFilter, которое заразило не менее 500 тыс. маршрутизаторов и устройств IoT. Продолжение кибератаки могло привести к срыву технологических процессов и возможной аварии [815]. Эксперты Ростелекома обнаружили двукратный рост числа хакерских атак на стратегические предприятия в России в 2020 году. Киберпреступники, как правило, пытались завладеть почтой топ-менеджеров предприятий и перехватить контроль над инфраструктурой. Рост такого рода атак на стратегические предприятия обусловлен переходом на удаленную работу сотрудников и образованием уязвимостей в информационной инфраструктуре. Центр мониторинга и реагирования на кибератаки Solar JSOC компании «Ростелеком-Солар» за январь – ноябрь 2020 года зафиксировал более 200 профессиональных хакерских атак на российские компании (двукратный рост по сравнению с 2019 годом), в том числе 30 атак со стороны группировок наиболее высокого уровня, работающих на

или недоступность услуг могут привести к значительным разрушениям и оказать негативное влияние на промышленное производство, безопасность жизни и имущества [816][62]. Данный сбой может распространиться на другие части, вызывая каскадные сбои во многих других связанных инфраструктурах с нарастающими негативными последствиями в экономике. В последние годы отмечается тенденция увеличения количества выявленных взломов систем управления критической инфраструктуры с целью вывода ее из строя либо шпионажа[63]. Реализация концепции Smart City сталкивается с угрозами безопасности под воздействием кибератак по причине хрупкости системы и широких возможностей для утечки данных [527, 817]. Кроме того, отмечается проблема информационных островов в случае расширения изоляции данных и несовместимости между различными системами и организациями [527][64].

иностранные государства. Чаще всего профессиональные группировки пытались взломать объекты критической информационной инфраструктуры: банки, атомные предприятия, объекты здравоохранения, электроснабжения, военные объекты и организации государственного управления (Где тонко, там и взломится. – Режим доступа: https://www.kommersant.ru/doc/4593929. – Дата доступа:01.12.2020). В мае 2021 года крупнейшую трубопроводную компанию США Colonial Pipeline атаковала группа хакеров DarkSide. Washington Post считает, что DarkSide – это группа хакеров из Восточной Европы. Трубопровод Colonial Pipeline проходит по побережью Мексиканского залива на юг и восток США. Паника вокруг атаки вызывала нехватку газа на юго-востоке и повысила обеспокоенность о растущей угрозе программ-вымогателей (Ransomware attack leads to shutdown of major U.S. pipeline system. – Режим доступа: https://www.washingtonpost.com/business/2021/05/08/cyber-attack-colonial-pipeline/. – Дата доступа: 08.05.2021). Атака на крупнейшего переработчика мяса в США – компанию JBS была совершена в 30.05.2021: из строя были выведены пять мясоперерабатывающих заводов, которые обеспечивают 25% национальных поставок говядины и 20% свинины. Выведя из строя заводы, хакеры потребовали выкуп – так же, как это было с атакой на Colonial Pipeline в мае, которая привела к перебоям с бензином и росту цен в 18 штатах.

[62] Неудачная кибератака на нефтехимический завод в Саудовской Аравии в августе 2017 г. была призвана не только сабботировать работу завода, но и вызвать взрыв, который мог привести к человеческим жертвам. Однако ошибка в компьютерном коде, использованном злоумышленниками, предотвратила взрыв. В октябре 2017 года DDoS-атаки на транспортную сеть в Швеции привели к задержке движения поездов [814].

[63] По данным исследования компании «Ростелеком-Солар», каждая десятая критически значимая информационная инфраструктура в России скомпрометирована вредоносным ПО. Речь идет о госорганах, банках, оборонных и транспортных объектах (Критически уязвимая инфраструктура. – Режим доступа: https://www.kommersant.ru/doc/4838304?tg. – Дата доступа: 03.06.2021).

[64] В Китае, где «умные города» начали развиваться после 2010 года, отмечена проблема обмена данными и интеграции. Например, в г. Нанкине из-за несовместимых форматов данных и стандартов между системами метро и автобусов местным органам власти пришлось понести дополнительные расходы в размере 100 млн юаней для их интеграции в рамках общей платежной системы.

Intellectual Transport Systems (умные траспортные системы) [365] в рамках концепции «Smart City» становятся все более интеллектуальными благодаря цифровым технологиям. Транспортные средства, оснащенные системами компьютерного зрения, различными видами датчиков и камер, обмениваются друг с другом информацией в режиме реального времени. В этой связи целостность данных является основной проблемой безопасности, связанной с безопасностью интеллектуальной транспортной системы.

Дальнейшая цифровизация сектора телекоммуникаций выражается в росте мошеннических операций с использованием поддельных идентификационных данных (например, банков, налоговых органов) для совершения нежелательных звонков и отправления сообщений, что приводит к финансовым потерям [733][65]. Одним из самых опасных с точки зрения потери финансовых ресурсов и затрагивающих как регулятора, так и поставщиков телекоммуникационных услуг, является мошенничество с обходом или мошенничество с SIM Box[66]. Данный вид преступлений распространен в регионах или странах, где тарифы на международную связь значительно выше, чем местные звонки на стационарный или мобильный номер. Мошенники размещают устройство SIM Box, которое позволяет перенаправлять вызовы от международного вызывающего к вызываемому абоненту, маскируя звонок как происходящий с местных мобильных или телефонных фиксированных станций, таким образом, обходя сборы, уплачиваемые регулятору за международный (междугородный) вызов.

Блокчейн интегрируется как в традиционные отрасли на базе концепций Industry 4.0, Smart Grid, Smart Chain Supply и прочих, так и, главным образом, FinTech-индустрию. Среди рисков внедрения данной технологии выделяют плохую защиту криптовалютной

[65] По данным Ассоциации по борьбе с мошенничеством в связи (Communications Fraud Control Association CFCA), в телекоммуникационной отрасли по всему миру накоплено около 2,25 трлн долларов убытков. [820]. Нежелательные звонки или спам-звонки позволяют мошенникам зарабатывать более 38 млрд долларов в год, что составляет около 1,69% общего дохода от телекоммуникаций. Основные категории мошенничества в телекоммуникационных сетях: фальсификация SMS (0,8 млрд долларов), фишинг и фарминг (1,6 млрд долларов США), атака обратного вызова (Вангири) (1,8 млрд долларов).

[66] В результате мошенничества среднегодовые убытки составляют 4,3 млрд долларов США (2017 Global Fraud Loss Survey. – Режим доступа:https://goo.gl/yh2uhu. Дата доступа: 08.02.2022).

индустрии, что создает потенциал для кражи криптовалютных активов пользователей, в особенности с применением специально разработанного вредоносного ПО [672]. Взломы как биржевых, так и криптовалютных кошельков стали более распространенными и масштабными как на уровне криптовалютных биржевых платформ[67], так и FinTech-организаций[68]. Согласно исследованию CipherTrace [818], в 2018 году с биржевых площадок было похищено 950 млн долларов (360% к уровню 2017 года). В отличие от регулируемых бирж, на большинство криптобирж не распространяются обычные требования к достаточности капитала, предусмотренные финансовым регламентом [819]. Большинство криптобирж мало капитализированы, и в случае нарушения безопасности эти биржи не покрываются страховкой и не имеют необходимых финансовых возможностей для покрытия потерь. По причине высокого инвестиционного риска и возможностей для мошенничества ряд юрисдикций, таких как Китай и Южная Корея, в 2017 году запретили ICO. Согласно отчету Ernst & Young за декабрь 2017 года, из общего объема средств, привлеченных ICO в размере 4 млрд долларов, около 10% похищены киберпреступниками [586].

---

[67] Основанная в 2010 году в Гонконге платформа обмена криптовалютами Bitfinex пострадала от серии кибератак, крупнейшая из которых привела к краже около 700 тыс. Биткоинов в 2014 году. Это составило около 473 млн долларов и является вторым по величине взломом обмена Биткойнов. В декабре 2017 года киберпреступники похитили Биткойны на сумму около 70 млн долларов у NiceHash, платформы для торговли цифровыми валютами, расположенной в Словении. В январе 2018 года киберпреступники взломали биржу криптовалют Coincheck Inc. и похитили около 530 млн токенов NEM. В сентябре 2020 года криптобиржа KuCoin сообщила о выводе Биткоинов, ERC-20 и других токенов с горячих кошельков биржи на сумму более 150 млн долларов (Взломана криптобиржа KuCoin, похищено более $150 млн в криптовалюте. – Режим доступа: https://whattonews.ru/vzlomana-kriptobirzha-kucoin-pohishheno-bolee-150-mln-v-kriptovaljute/. – Дата доступа: 03.11.2021). Российская криптовалютная биржа Livecoin в декабре 2020 года объявила о закрытии после резкого прекращения операций (After alleged hack, Russian crypto exchange Livecoin shuts down. – Режим доступа: https://cointelegraph.com/news/after-alleged-hack-russian-crypto-exchange-livecoin-shuts-down. – Дата доступа: 18.01.2021). Биржа подверглась спланированной атаке, в результате которой она потеряла контроль над всеми своими серверами. В рамках инцидента хакерам удалось захватить инфраструктуру Livecoin и изменить цены на бирже до аномально высоких значений.

[68] DAO была основана как организация венчурного капитала на основе Ethereum, которая позволяла создавать и внедрять DApps (децентрализованные приложения) на своей платформе. В мае 2016 года краудфандинг для DAO привлек более 150 млн долларов. Программный изъян DAO позволил кибер-преступникам украсть 50 млн долларов.

Вместе с тем, как показали результаты исследования CipherTrace, в 2020 году значительно сократилось число преступлений, связанных с криптовалютной индустрией [821]. Аналитики определили, что данный показатель снизился на 57% в 2020 году. Объем криминальных операций в криптосфере сократился ориентировочно до 1,9 млрд долларов[69]. В 2019 году незаконная деятельность составила 2,1% от всего объема транзакций с криптовалютой, или около 21,4 млрд долларов переводов. Вместе с тем в 2020 году доля незаконных операций с криптовалютой упала до 0,34%, или 10,0 млрд долларов в объеме транзакций [822].

Инструментарий банковских кибератак предполагает использование вредоносных программ (включая банковские троянские программы[70]) и различных специализированных форм кибератак (включая DDoS[71]), направленных на уязвимость системы онлайн-банкинга [726, 823, 824, 825][72].

Так, согласно отчету Лаборатории Касперского за 2021 год [826], выделяются следующие киберугрозы в банковской сфере:

1) перепродажа доступа к банковским системам[73];

2) атаки программ-вымогателей на банковские сети[74];

---

[69] Например, в 2019 году преступники совершили с цифровыми активами сделки на общую сумму до 4,5 млрд долларов.

[70] TrickBot – это первый и единственный банковский троян, предназначенный для клиентов крупных банков, которые охватывают множество географических и языковых зон по всему миру. Сначала TrickBot предназначался для финансовых учреждений, расположенных в Великобритании, Австралии и Швейцарии. В настоящее время операторы TrickBot проводят свои атаки перенаправления против банков в 19 разных странах [827].

[71] Финансовый ботнет – это распределенная сеть зараженных компьютеров, которой можно удаленно управлять с одного и того же сервера управления и контроля с целью атаки на финансовых клиентов [828].

[72] В результате кибератаки на банк JPMorgan Chase в 2016 году было взломано около 76 млн учетных записей. DDOS-атака на HSBC в 2018 году привела к двухдневному простою в системах онлайн-банкинга данного кредитного учреждения [615]. В 2021 году мошенничество с интернет-банкингом в Великобритании выросло на 117% по объему и на 43% по стоимости в сравнении с уровнем 2020 года [726].

[73] Существует рынок предложений по удаленному доступу к различным банковским системам по всему миру. Как правило, кибер-преступники получают доступ через уязвимости, а затем перепродают его злоумышленникам, преследующим свои финансовые интересы, например операторам программ-вымогателей.

[74] Различные группы вымогателей проводили целевые атаки на банки по всему миру, например в Коста-Рике, Чили и на Сейшельских островах. Эти три случая широко освещались СМИ. За атаки в Коста-Рике несет ответственность группа Maze, а за атаками в Чили стояла группа REvil (Sodinokibi). При этом жертва нападения, заплатившая выкуп, не появляется в списке организаций, подвергшихся атаке.

3) разработка специального программного обеспечения для атаки коммерческих VPN-провайдеров и устройств, работающих в инфраструктуре их клиентов. Кроме того, злоумышленники создавали микропрограммы для сканирования сетей и сбора данных;

4) заражение интернет-банков троянцами[75];

5) атаки финансовых приложений, включая приложения криптовалютных бирж[76];

6) кража данных платежных карт[77];

7) вредоносное программное обеспечение для атак на POS-терминалы и банкоматы[78].

По данным Сбербанка России, ежедневно фиксируется более 100 кибератак на инфраструктуру и финансовые сервисы банка, совершается более 10 тыс. попыток мошенничества в отношении клиентов [829]. В 2021 году зафиксирована «самая мощная в мире атака на финансовый сектор» распределенного типа DDoS на 12 крупных финансовых организаций России, а также процессинговые компании и Интернет-провайдеры. Для увеличения мощности атаки кибепреступниками использовалась инфраструктуры IoT [830].

Согласно данным Центрального банка России, во втором квартале 2021 года объем операций без согласия клиентов выросла по сравнению с аналогичным периодом 2020 года на 23%, при этом объем украденных средств превысил 3 млрд российских рублей (рост на 38%) [831]. При этом среди типов цифровых атак доминируют атаки с элементами социальной инженерии и фишинговые атаки. Среди стран, подвергшихся значительным кибератакам 2006–2020 годах лидируют США, Великобритания, Индия, ФРГ и Ю. Корея.

С учетом выявленных угроз и ограничений современных технологических решений, на уровне отраслей интеграция цифровых концептов генерирует, в том числе, следующие риски (табл. 2.5).

---

[75] Примерами, подтверждающими данную тенденцию, являются такие программы, как Ginp, Ghimob, Anubis и Basbanke.

[76] Примером является семейство Ghimob.

[77] Примером являются атаки Magecart 3.0.

[78] Группа Prilex, распространяющая вредоносное ПО по модели MaaS, начала перехватывать данные, которыми обмениваются платежные терминалы. Вредоносное программное обеспечение CESSO стало предоставляться как услуга для атак на банкоматы Diebold, Wincor и NCR и кражи денежных средств в евро, долларах США, валютах латиноамериканских стран.

Таблица 2.5

Риски и угрозы цифровизации на уровне отраслей
(разработано автором на основе [21, 211, 365, 411, 527, 760, 809, 812, 814, 817, 832–839])

Концепты	Промышленность	Финансовый сектор	Энергетика	Сельское хозяйство	Транспорт и логистика	Торговля	Коммунальное хозяйство
RGTS	–	Сбой по причине эндогенных или экзогенных факторов несет прямые финансовые убытки в банковском секторе	–	–	–	–	–
FinTech	–	Прямые финансовые потери от взлома и хищения криптоактивов криптобирж, мошенничество при ICO, кража персональных данных, цифровых данных платежных карт, атаки POS-терминалов и банкоматов	–	–	–	–	–

Продолжение табл. 2.5

Концепты	Промышленность	Финансовый сектор	Энергетика	Сельское хозяйство	Транспорт и логистика	Торговля	Коммунальное хозяйство
Industry 4.0	Кибератаки (DDos), блокировка систем управления производством, кража фальсификация коммерческой информации, интеллектуальной собственности, шпионаж. Атаки на промышленное оборудование, включая роботов, приводят к росту рисков в отношении промышленных активов, финансовых показателей, бизнес-репутации, жизни и здоровья работников, пользователей[79] и потребителей[80]	–	–	–	Нарушение функциональной работы цепочек поставки[81]	Взлом коммерческой информации о покупателях продукции и поставщиках	–
Agricul-ture 4.0	–	–	–	Сбой систем может привести к прямым финансовым убыткам и сокращению с.-х. производства	–	–	–

Продолжение табл. 2.5

Концепты	Промышленность	Финансовый сектор	Энергетика	Сельское хозяйство	Транспорт и логистика	Торговля	Коммунальное хозяйство
Smart Grid	Дестабилизация энергетической системы вызывет каскадный негативаный эффект в промышленности	–	Скоординированные кибератаки[82], которые могут одновременно нацеливаться на достаточное количество критически важного энергогенерирующего оборудования, чтобы вызвать каскадные эффекты и в конечном итоге привести к краху энергосистемы; программ-вымогателей, которые препятствуют стабильной работе системы и осуществлению энергопередачи; кибератаки приводят к нарушению работы подстанций и прекращению обслуживания клиентов	–	–	–	–

Продолжение табл. 2.5

Концепты	Промышленность	Финансовый сектор	Энергетика	Сельское хозяйство	Транспорт и логистика		Торговля
Smart Supply Chain	Сбои систем транспорта и логистики приведут к срыву поставок, возможной остановке производства и финансовым убыткам	–	–	–	Сбои систем транспорта и логистики приведут к финансовым убыткам		–
E-Commerce	–	–	–	–	–	Сбои систем приведут к сокращению объемов торговли, прямым финансовым убыткам	–
Smart City	–	–	–	–	–	–	Кибератаки диспетчерских систем приведут к сбоям в работе всей системы, нарушая целостность обмена информацией и конфиденциальность цифровых данных пользователей

Окончание табл. 2.5

Концепты	Промышленность	Финансовый сектор	Энергетика	Сельское хозяйство	Транспорт и логистика	Торговля	Концепты
Intellec-tual Transport Systems VANET	–	–	–	–	Изменение цифровых данных в автономных транспортных средствах может привести не только к имущественному ущербу, но и физической угрозе водителей и пешеходов[83]	–	–

[79]Аддитивное производство имеет ряд уязвимостей, связанных с технологией АМ, усугубляемой ее цифровой природой, может потенциально позволить злонамеренным агентам вносить внутренние дефекты, такие как поры или внутренние геометрические неточности, ставя под угрозу механические и функциональные свойства продукта, без возможности их обнаружения традиционными методами квалификации [840]. В то же время очень важно учитывать потребности, связанные с задачами проектирования и проверки киберфизических систем [841].

[80] Механические детали внутри роботов, такие как захваты, двигатели, шестерни, колеса или поршни, которые позволяют роботам перемещать, захватывать и поднимать предметы, представляют серьезную угрозу, если ими управляют злоумышленники.

[81] Такие предприятия, как Fiat, Chrysler, T-Mobile USA, IRS, CVS, Costco, Бостонский медицинский центр и другие, пострадали от кибератак по причине взлома их сторонних поставщиков.

[82] Кибератаки на критическую инфраструктуру классифицируются на четыре основных типа: атака на устройства, атака на цифровые данные, атака на конфиденциальность и сетевая атака [814, 836, 837]: а) атака на устройства направлена на компрометацию

и управление сетевым устройством. Часто это начальный этап крупной атаки, когда одно взломанное устройство используется в качестве точки входа для запуска дальнейших атак и взлома остальной части интеллектуальной сети (например, скомпрометированный датчик может использоваться для отправки вируса, замаскированного под подлинные данные обнаружения, и, следовательно, распространения его по остальной части сети и заражения всей сети); б) атака на цифровые данные направлена на незаконное изменение или удаление цифровых данных или команды управления в трафике сети связи, чтобы ввести в заблуждение систему управления для принятия неправильных решений или действий (например, когда клиент манипулирует интеллектуальным счетчиком, чтобы изменить свои данные о потреблении, отразить меньшие суммы в своем счете за электроэнергию); в) атака на конфиденциальность направлена на извлечение персональной информации пользователей; г) сетевая атака, как правило, осуществляется в форме отказа в обслуживании (DoS) и направлена на использование или перегрузку коммуникационных и вычислительных ресурсов сети критической инфраструктуры. В декабре 2015 года хакерам удалось захватить контроль над подключенной системой управления энергосистемой Украины, успешно взломав систему надзора и сбора данных (supervisory control and data acquisition SCADA) сети с помощью вредоносного ПО BlackEnergy. Это вызвало массовое отключение электроэнергии, в результате которого более 700 тыс. человек остались без электричества на несколько часов [842]. В июле 2017 года была атакована электрическая сеть, которая поставляет электроэнергию, в Великобритании и Ирландии. Кибератака была направлена на проникновение в системы управления питанием, чтобы они могли отключить всю или часть электросети. Это было сделано с использованием поддельных электронных писем, предназначенных для некоторых старших сотрудников энергетической компании. Электронные письма содержали техническую информацию об умной сети, предназначенную для того, чтобы выдавать их за подлинную почту, но на самом деле предназначались для незаконной информации или для того, чтобы пользователи нажимали на ссылки для запуска вредоносного программного обеспечения в так называемой фишинг-атаке.

[83] В специализированной литературе [843, 844] кибератаки на системы VANET подразделяют на активные и пассивные в зависимости от их характера. Активные атаки – это те, в которых злоумышленник активно участвует в атаке для извлечения конфиденциальной информации из сети. В случае пассивной атаки злоумышленник пассивно собирает информацию о сети, не вмешиваясь в нее и не вводя какую-либо информацию в сеть. Раскрытие идентификационных данных является примером пассивной атаки.

Таким образом, с учетом специфики внедряемых цифровых систем на уровне отраслей представляется возможным сформировать следующую матрицу киберугроз в зависимости от секторов (табл. 2.6).

Таблица 2.6

Эмпирические оценки рисков и угроз по основным видам кибератак по методологии CIA (разработано автором)

Название атаки	Узел атаки	Отрасль, сфера деятельности либо экономики	Уровень риска взлома и сопутствующего ущерба в работе предприятий		
			Низкий	Средний	Высокий
АЗС – атака захвата сеанса, при которой злоумышленник влияет на сеанс связи между узлами / транспортными средствами	Системы IoT	Industry 4.0, Smart City, Intellectual Transport Systems, Smart Grid			–
АИЭЗ – атака на инфраструктуру электронного здравоохранения	Информационные системы	Здравоохранение			–
АИСИ – атака с использованием методов социальной инженерии	Личные данные клиентов и работников предприятий и организаций	Финансовая и страховая деятельность, сектор ИКТ, оптовая и розничная торговля, государственное управление и оборона, обязательное социальное обеспечение		–	–
АКИ – атака на критическую инфраструктуру с использованием широкого перечня инструментария	Информационные и производственные системы объектов критической ифраструктуры	Промышленность, энергетика, системы жизнеобеспечения, информационные и телекоммуникационные системы, банковская система, транспортная система, информационные системы органов государственного управления, здравоохранение			–

Продолжение табл. 2.6

Название атаки	Узел атаки	Отрасль, сфера деятельности либо экономики	Уровень риска взлома и сопутствующего ущерба в работе предприятий		
			Низкий	Средний	Высокий
АП – атака через посредника (Man in the Middle), предполагающая размещение злоумышленника между двумя взаимодействующими законными узлами (транспортными средствами), подслушивающего их связь, вводящего ложную информацию или изменяющего сообщение между ними	Системы IoT	Industry 4.0, Smart City, Intellectual Transport Systems, Smart Grid			–
АПР – атака на промышленных роботов	Системы управления оборудованием	Industry 4.0			–
АРИИ – атака раскрытия идентификационной информации	Базы данных	Банковский сектор, сектор ИКТ, органы государственного управления, системы здравоохранения, Smart City, Intellectual Transport Systems, E-Government		–	
АЦП – атака цепочки поставок	Данные о поставщиках и клиентах	Промышленность, транспорт, Smart Supply Chain		–	
АЧ – атака червоточины, при которой два вредоносных узла участвуют в сети для создания частного туннеля, называемого червоточиной, где первый вредоносный узел на одном конце передает данные второму вредоносному узлу на другом конце, что приводит к нарушению безопасности для пакетов	Системы IoT	Industry 4.0, Smart City, Intellectual Transport Systems	–	–	

Продолжение табл. 2.6

Название атаки	Узел атаки	Отрасль, сфера деятельности либо экономики	Уровень риска взлома и сопутствующего ущерба в работе предприятий		
			Низкий	Средний	Высокий
АЧД – атака черная дыра, при которой злоумышленник обманывает протокол маршрутизации, представляя себя как узел с кратчайшим путем к узлу назначения, таким образом, вместо того, чтобы полагаться на процесс обнаружения маршрута, все узлы начинают доверять поддельному маршруту и в конечном итоге пакеты данных перехватываются вредоносным узлом	Системы IoT	Industry 4.0, Smart City, Intellectual Transport Systems, Smart Grid	–	–	
ВП – вредоносные программы, такие как черви, вирусы, трояны, вымогатели, бэкдоры, шпионское ПО и т. д.	Информационные системы, базы данных	Промышленность, энергетика, строительство, водоснабжение, финансовый сектор, сектор ИКТ, транспортный сектор, торговля, системы государственного управления, образование, здравоохранение, Smart City, Intellectual Transport Systems, CBDC, E-Government			–
ВБК / ВКК – взлом биржевых и криптовалютных кошельков	Инфраструктуры криптовалют	FinTech	Криптокошельки криптобиржи		Криптокошельки CBDC
ДТ – двойная трата, предполагающая возможность пользователю выполнять несколько транзакций с одной и той же криптовалютой)	Инфраструктуры криптовалют	FinTech			
ИПИД – использование поддельных (краденых) идентификационных данных	Платежные, сервисные системы	FinTech, RTGS, банковский сектор, сектор ИКТ, цифровые системы государственного управления, E-Government			

Продолжение табл. 2.6

Название атаки	Узел атаки	Отрасль, сфера деятельности либо экономики	Уровень риска взлома и сопутствующего ущерба в работе предприятий		
			Низкий	Средний	Высокий
ККиС – коммерческий кибершпионаж и саботаж с целью получения коммерческих секретов и конкурентного преимущества	Базы данных	Промышленность, банковский сектор, сектор ИКТ, транспорт и логистика, торговля			
Кр – криптоджекинг, предполагающий несанкционированное использование чужих компьютеров для майнинга криптовалюты	Сетевое оборудование	FinTech			
КЦД – кража цифровых (личных) данных	Базы данных	Промышленность, банковский сектор, сектор ИКТ, торговля, системы государственнного управления, образование, здравоохранение, E-Government, Smart City, Intellectual Transport Systems, Smart Grid, FinTech			
М – использование сервисов (миксеров) с целью скрытия взаимосвязи между адресами в последовательных транзакциях, скрытия владельцев криптоактивов и их происхождения	Крипторынки	FinTech			
МА – маскарадная атака, предполагающая маскировку злоумышленником своей личности, чтобы действовать в качестве легитимного узла с намерением генерировать ложные сообщения в сети или модифицировать полученное сообщение	Системы IoT	Industry 4.0, Smart City, Intellectual Transport Systems, Smart Grid			

Продолжение табл. 2.6

Название атаки	Узел атаки	Отрасль, сфера деятельности либо экономики	Уровень риска взлома и сопутствующего ущерба в работе предприятий		
			Низкий	Средний	Высокий
MAP – атака маршрутизации, предполагающая перехват сообщений в сети Блокчейн	Инфраструктура Блокчейн	FinTech			
MO – мошенническая операция	Платежные системы и сервисы	Банковский сектор, FinTech, Smart Grid, E-Commerce, CBDC			
MOSIM – мошенничество с обходом или мошенничество с SIM	Биллинговые системы	Сектор ИКТ			
ПАТ – прослушивание и анализ трафика	Системы IoT	Smart City, Intellectual Transport Systems			
ПВSCADA – программы взлома систем управления производством	Производственные системы	Промышленность, энергетика, водоснабжение			
ПИА – поддельная информационная атака, направленная на передачу ложной информации по сети	Системы IoT	Smart Supply Chain, Smart Grid, Industry 4.0, Smart City, Intellectual Transport Systems			
ПУОИ – потеря управления при использовании облачной инфраструктуры	Облачная инфраструктура	Промышленность, энергетика, банковский сектор, сектор ИКТ, транспорт, торговля, системы государственного управления, здравоохранение, FinTech			
УАИ – узловая атака имитации, направленная на нарушение аутентификации в сети	Системы IoT	Industry 4.0, Smart City, Intellectual Transport Systems, Smart Grid			
УАСУ – удаленная атака на системы управления трафиком с поддержкой Интернета вещей	Системы IoT	Industry 4.0, Smart City, Intellectual Transport Systems, Smart Grid			
ФА(0) – фишинговая атака, целью которой является объект критической инфраструктуры	Сетевые системы, базы данных	Промышленность, энергетика, водоснабжение, финансовый сектор, сектор ИКТ, транспортный сектор, торговля, системы государственного управления, образование, здравоохранение, Smart City, Intellectual Transport Systems, Smart Grid			

Продолжение табл. 2.6

Название атаки	Узел атаки	Отрасль, сфера деятельности либо экономики	Уровень риска взлома и сопутствующего ущерба в работе предприятий		
			Низкий	Средний	Высокий
ФА(1) – фишинговая атака, целью которой является юридическое лицо					
ФА(2) – фишинговая атака, целью которой является клиент юридического лица					
ЭУПО – эксплуатация уязвимостей ПО	Информационные системы	Промышленность, энергетика, водоснабжение, финансовый сектор, сектор ИКТ, транспортный сектор, торговля, системы государственного управления, образование, здравоохранение, Industry 4.0, Intellectual Transport Systems, Smart Grid			
APT – целевая кибератака	Информационные системы	Промышленность, энергетика, водоснабжение, финансовый сектор, сектор ИКТ, системы государственного управления, здравоохранение, Smart City, Intellectual Transport Systems			
DDoS-атаки, генерирующие избыточный трафик, что препятствует доступу пользователей к ресурсу или услуге	Сетевые системы	Энергетика, финансовый сектор, сектор ИКТ, транспортный сектор, торговля, системы государственного управления, образование, здравоохранение, Industry 4.0, Smart City, Intellectual Transport Systems			

Окончание табл. 2.6

Название атаки	Узел атаки	Отрасль, сфера деятельности либо экономики	Уровень риска взлома и сопутствующего ущерба в работе предприятий		
			Низкий	Средний	Высокий
Eclipse-атака, предполагающая изоляцию конкретного узла одноранговой сети с целью получения контроля всех исходящих соединений узла	Инфраструктура Блокчейн	FinTech			
GPS-атака, направленная на взлом управления положением транспортных средств с помощью имитаторов GPS, которые выдают более сильные сигналы, чем исходная спутниковая система GPS	Инфраструктура IoT	Smart City, Intellectual Transport Systems			
Sybil-атака узла IoT, при которой используются несколько идентификаторов для компрометации основной части сети	Инфраструктура IoT, криптосфера	Smart City, Intellectual Transport Systems, FinTech			

В настоящее время, как показал проведенный анализ, среди наиболее распространенных и опасных инструментов кибератак выделяют вредоносные программы (ВП), целевые кибератаки (APT) и DDos атаки.

1. Вредоносные программы, такие как черви, вирусы, трояны, вымогатели, бэкдоры, шпионское ПО и т. д., использовались мошенниками для организации атак на компьютерные системы с целью нарушения конфиденциальности, целостности передаваемых данных и доступности услуг, предлагаемых базовой инфраструктурой[84] [726, 845].

При этом, как показал ряд исследований, выделяют следующие тенденции распространения вредоносных программ [832]:

а) существенно возрастает сложность вредоносных программ;

[84] Отчет Лаборатории Касперского за 2015 год показал, что из-за атак вредоносных программ за два года из финансовых учреждений всего мира было украдено до 1 млрд долларов. Количество вредоносных программ увеличилось на 358% в 2020 году, а количество программ-вымогателей возросло на 435%, при этом общая стоимость криптовалюты, полученная по адресам программ-вымогателей, увеличилась в четыре раза [726].

б) цели атаки смещаются в сторону сложного шпионажа;

в) векторы доступа становятся комплексными и зависимыми от наличия уязвимости нулевого дня[85];

г) в ближайшем будущем кибератаки станут более распространенными и разрушительными;

д) таргетированному шпионскому вредоносному программному обеспечению не хватает модулей для киберфизических атак и специальных протоколов интеллектуальных сетей, однако такие функции будут реализованы в будущем.

Одним из самых распространенных инструментов кибератак являются программы-вымогатели[86]. Исследования показывают, что в 2014–2017 годах было выявлено 327 семейств вымогателей, в результате которых было совершено 184 млн атак [846]. Цифровая бизнес-платформа Statista оценивает количество атак программ-вымогателей в 2020 году в размере 304 млн единиц, при этом рост по сравнению с 2019 годом составил более 60% [847]. В 2020 году экономические потери от программ-вымогателей составили около 20 млрд долларов [822, 853]. Общая стоимость криптовалюты, полученной преступными организациями в 2020 году, по данным [822], составила около 10 млрд долларов.

В 2018 году 40% средних и крупных британских компаний подвергались в среднем пяти атакам программ-вымогателей, суммарные выплаты каждой организации превысили 320 тыс. фунтов стерлингов в год [848]. Важно отметить, что около 90% предприятий, потерявших данные, были вынуждены прекратить бизнес-деятельность в течение следующих двух лет после атаки.

Как показало исследование Лаборатории Касперского, секторально наиболее подверженными отраслями данного вида кибератак являются образование, ИКТ, медиа и развлечения, финансовые услуги, медицинские учреждения[87]. Согласно отчету Chainalysis 2021,

---

[85] 0-day (zero day) – термин, обозначающий неустраненные уязвимости, а также вредоносные программы, против которых еще не разработаны защитные механизмы.

[86] Вредоносное программное обеспечение, которое после загрузки в систему-жертву шифрует жесткий диск и требует выплаты выкупа.

[87] Больницы и иные медицинские учреждения становятся мишенями программ-вымогателей, так как для них доступ к файлам с данными пациентов является критическим. Медицинские учреждения, как правило, не располагают ни финансовыми, ни людскими ресурсами, необходимыми для организации и поддержания надлежащей киберзащиты [783]. В мае 2017 года программа-вымогатель (WannaCry) заразила более 300 тыс. компьютеров, в том числе ряд высокопроизводительных систем, включая Национальную службу здравоохранения Великобритании (NHS) [846].

программы-вымогатели представляют собой серьезную растущую проблему кибербезопасности как для государственного, так и для частного сектора [849]. Известные выплаты злоумышленникам-вымогателям с 2019 года по 2020 год выросли на 337% и достигнули суммы более 400 млн долларов. Отмечается, что приведенные данные – это нижние оценки, реальные показатели выше. При этом средний размер выкупа значительно вырос с 12 тыс. долларов в криптовалюте в четвертом квартале 2019 года до 54 тыс. долларов в первом квартале 2021 г. Данная тенденция объясняется повышением эффективности атак более крупных организаций с помощью незаконного приобретения инструментов для взлома, украденных данных и других цифровых активов. По мнению экспертов Chainalysis, самое большое количество атак с использованием программ-вымогателей осуществляется киберпреступниками из СНГ.

2. Целевые кибератаки[88] (APT) предполагают скрытое внедрение в ИТК-сектор организации, как правило, с целью кражи данных и промышленного шпионажа. Целевые атаки иногда остаются необнаруженными в течение месяцев или даже лет[89] [850]. Согласно исследованию Symantec [819], вредоносная программа Stuxnet заразила около 100 тыс. систем в 115 странах; программа Duqu, предназначенная для промышленных систем управления, собирала конфиденциальную информацию по крайней мере в 8 странах[90] [852, 853].

3. DDoS-атаки, имеет целью отключение компьютерных систем или сетей[91] [854]. По мнению Европейского полицейского

[88] Целевые кибератаки позволяют создавать возможности для достижения целей посредством различных векторов нападения (например, информационных, физических и обманных). Эти цели обычно включают установление и расширение своего присутствия внутри информационно-технологической инфраструктуры целевой организации для осуществления намерений извлечения информации, срыва или создания помех критическим аспектам выполняемой задачи, программы или службы.

[89] Главный пример – Stuxnet, который предназначался для программируемых логических контроллеров чувствительных промышленных систем, был активен в течение по крайней мере 3 лет до открытия [851].

[90] С точки зрения шпионажа троян Regin, как полагают, использовался для глобальных систематических кампаний как минимум с 2008 года.

[91] DoS – отказ в обслуживании; атаки DoS с происхождением из нескольких источников называются атаками распределенного отказа в обслуживании – DDoS.

управления (Европол) [855], инструментарий DDoS становится все более связанным с организованной преступностью. Ведущий поставщик решений для сетевой защиты компания Corero Networks [734] подтвердила, что сетевые атаки, такие как распределенный отказ в обслуживании (DDoS), в год увеличиваются на 40%[92], достигнув в 2018 году более чем 400 тыс. атак в месяц[93] .

Специфика использования кибератак различного вида в отношении экономических, социальных и общественных объектов воздействия позволяет провести следующий сравнительный анализ их характеристик (табл. 2.7).

Таблица 2.7

Сравнительный анализ характеристик различных киберинструментов и их потенциальной направленности по секторам и сегментам экономики (разработано автором)

Характеристики киберинструментов	Вредоносные программы	APT-атаки	DDoS-атаки
Уровень охвата атакуемых объектов	Широкий	Узкий	Широкий
Сегрегация по секторам и сегментам атаки	Низкая	Высокая	Средняя
Зависимость от наличия внутренних и (или) внешних уязвимостей атакуемых объектов	Высокая	Специальная*	Низкая
Стоимость подготовки и реалзиации кибератаки	Низкая или средняя (в зависимости от конкретного инструмента)	Высокая	Высокая
Длительность предварительной подготовки	Низкая или средняя (в зависимости от конкретного инструмента)	Высокая	Средняя

[92] DDoS attacks in Q3 2018. – Режим доступа: http://goo.gl/ArpLPh. – Дата доступа: 31.10.2018.

[93] DDoS Attacks Increase 40% Year on Year Confirms Corero Networks. – Режим доступа: http://goo.gl/LxXT3w . – Дата доступа: 12.09.2018.

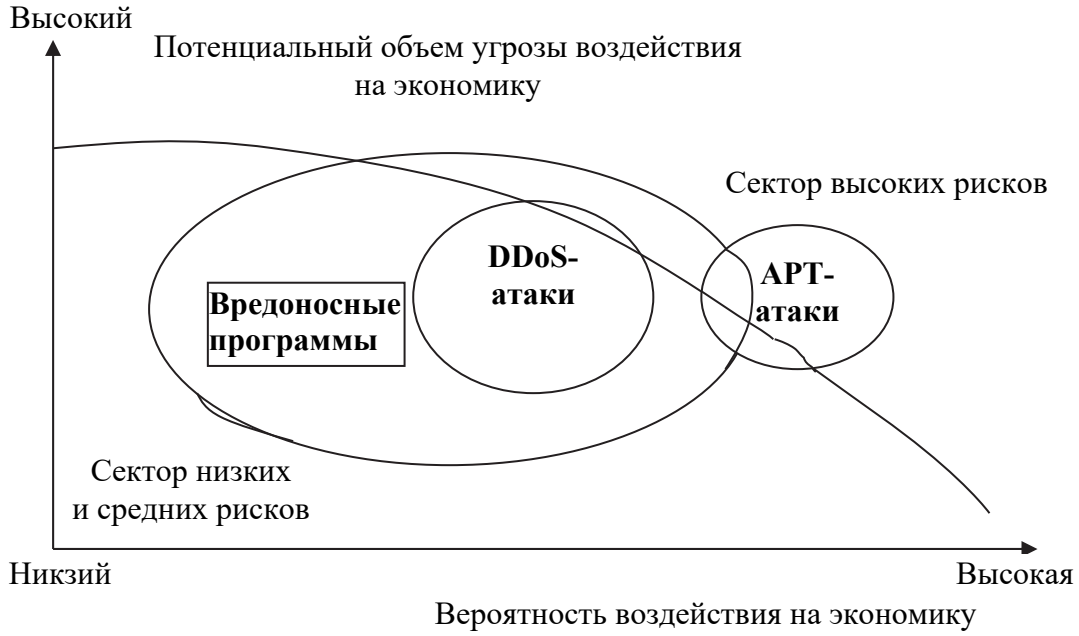
Окончание табл. 2.7

Характеристики киберинструментов	Вредоносные программы	APT-атаки	DDoS-атаки
Потенциальная направленность по секторам и сегментам экономики	Широкий спектр отраслей и сегментов экономики, включая компании сектора ИКТ, МСП, промышленные компании с низкой степенью киберзащиты и высокой степенью цифровизации бизнес-процессов, сектор государственного управления, медицинские учреждения, финансовые организации, образовательные учреждения, управление критической инфраструктурой	Узкий сектор наиболее защищенных в цифровом плане секторов и сегментов экономики, включая крупные IT-компании, банковские учреждения, органы государственного управления, промышленные предприятия сектора ВПК, управление критической инфраструктурой	Ограниченный перечень компаний, секторов и сегментов экономики, чьи бизнес-операции (специфика функционирования) предполагают необходимость нахождения онлайн в режиме 24/7, например сервисные услуги компаний, онлайн сервисы органов государственного управления, компании ИКТ, медицинские учреждения и спасательные (специальные) службы

* Предполагает длительную детальную подготовку (разведку) с целью выявления уязвимостей систем или персональных данных.

При использовании методологии McKinsey [795] представляется возможным построить следующую кривую распределения рисков на уровне экономики для различных киберинструментов (рисунок). Как показано на рисунке, в секторе особых рисков для макроэкономики находятся все инструменты кибератак, одноко воздействие различается. Наибольшая вероятность ущерба и уязвимости объектов для стабильности национальной экономической системы исходит от APT-атак, нацеленных на наиболее крупные и значимые индивидуальные объекты инфраструктуры и управления. DDoS-атаки нацелены главным образом на специфические сегменты бизнеса и управления, поэтому на уровне компаний их воздействие не является критическим. Вместе с тем в случае атаки государственных инфраструктурных объектов и систем управления ущерб может быть серьезным (с учетом косвенных, репутационных

и вторичных издержек). Вредоносные программы являются наиболее распространенным инструментом киберпреступлений, однако средняя вероятность прорыва систем защиты и отсутствие фокуса в отношении объектов воздействия делает этот инструментарий менее критическим, чем APT, но более значимым по сравнению с DDoS-атаками.



Распределение рисков на уровне экономики для различных киберинструментов (разработано автором)

В этой связи важно отметить расширение использования кибератак, спонсируемых государствами и организованными преступными группировками [757]. Злоумышленники (хакеры) имеют доступ к сложным инструментам, конфиденциальной информации и учетным данным (некоторые из них получены незаконным путем), финансовые ресурсы для субсидирования усилий в течение неограниченного периода времени и иммунитет от государственного преследования, возможно, даже степень анонимности или защиты личности [856].

К основным направлениям данного вида угроз следует отнести следующие:

1) атака критической инфраструктуры[94] [487];

[94] В 2007 году Эстония (правительственные учреждения, средства массовой информации и новостные порталы, банки и телекоммуникационная инфраструктура) подверглась кибератаке (DDoS-атаке), спонсируемой иностранным государством. Результатом стало размещение НАТО Центра передового опыта в области киберзащиты (CCDCOE) в г. Таллине [857, 858].

2) использование APT для кражи военных секретов или разведывательных данных;

3) коммерческий кибершпионаж и саботаж для получения коммерческих секретов, конкурентного преимущества по сравнению с конкурирующими бизнесами[95];

4) атака с целью получения доступа к личной компрометирующей и финансовой информации;

5) хакерские атаки или DDoS-атаки во имя «социальной справедливости» и (или) «возмездия» в отношении отдельных организаций[96];

6) инсайдерские угрозы, создаваемые недовольными сотрудниками, включающие использование доступа к внутренней системе и учетным данным или «социальную инженерию» для получения конфиденциальной информации;

7) деятельность одиночных хакеров по взлому военной инфраструктуры или инфраструктуры национальной безопасности;

8) кража финансовых активов в интересах конкретных государств[97].

При этом, по данным Лаборатории Касперского, наибольшее количество кибератак на компьютеры пользователей в ноябре 2019 – октябре 2020 годов происходило из США (49,8%), Нидерландов (13,36%), Франции (7,20%).

Следует отметить, что, согласно исследованию McKinsey, воздействие кибератак на различные сектора экономики является

---

[95] Правительство США в 2019 году запретило продажу продуктов Huawei своим клиентам, так как считает, что КНР установило «скрытые программы» в устройствах. Продукты от Checkpoint израильской компании также были запрещены для продажи правительственным клиентам США, поскольку Checkpoint не позволяла проводить проверку своего программного обеспечения [859].

[96] Хакерские коллективные группы, такие как Lulzsec или Anonymous, нацелены на веб-сайты или критически важную инфраструктуру и вызывают перебои в обслуживании и простои с соответствующими финансовыми и репутационными издержками.

[97] Эксперты по кибербезопасности выяснили, что в 2019–2020 годах хакеры КНДР украли в Биткоин и остальных криптовалютах около 316 млн долларов. Об этом сообщило агентство Kyodo, сославшись на отчет Комитета при Совбезе ООН по контролю за соблюдением санкций в отношении Пхеньяна. Исследователи выяснили, что хакеры взламывали не только криптовалютные биржи, но и сайты инвестиционных компаний и фондов. Даже частные трейдеры периодически становились жертвами корейских киберпреступников. За два года корейские хакеры украли более 300 млн долларов в криптовалюте (За два года корейские хакеры украли более $300 млн в криптовалюте. – Режим доступа: https://whattonews.ru/za-dva-goda-korejskie-hakery-ukrali-bolee-300-mln-v-kriptovaljute/. – Дата доступа: 10.02.2021).

неравномерным. В наибольшей степени им подвержены такие отрасли, как аэрокосмическая, фа рмацевтика, производство телекоммуникационного оборудования, химическая и производство IT-оборудования, которые относятся к инновационным отраслям экономики [860].

Анализ современных тенденций развития киберпреступлений и противодействия им позволяет отметить тот факт, что в условиях глобальной цифровизации формируется новая индустрия «киберпреступление как услуга» (CaaS) [733, 861]. При этом отдельно выделяются направления аутсорсинга предложения услуг «программа-вымогатель как услуга» (RaaS) и аренда бот-сетей для создания инфраструктуры DDoS-атак. Также выделяют следующие составляющие цифровизации криминальных услуг [862]:

а) обслуживание криминальной инфраструктуры, предполагающее предоставление серверов, необходимых для совершения киберпреступлений[98] [863];

б) предоставление услуг, включающих проектирование, создание и распространение вредоносных программ [864];

в) предоставление сервисов взлома, начиная с учетных записей электронной почты или социальных сетей, запуск DDoS-атак [863];

г) продажа личных, финансовых данных, информации об уязвимостях программ или приложений[99];

д) оказание услуги по отмыванию денег[100];

е) расширение в Интернете продажи наркотиков, оружия и поддельных ценных бумаг в период пандемии, кроме того, взрывной рост фишинговых ресурсов[101] [869];

---

[98] Вместо того чтобы рисковать совершением незаконных действий на своих компьютерах, правонарушители предпочитают либо подключаться к выделенному серверу или прокси-серверу, либо обращаться к услугам хостинга, чтобы избежать обнаружения правоохранительными органами. Хостинг-провайдеры играют решающую роль в криминальной онлайн-экономике, и услуги пуленепробиваемого хостинга являются одним из самых востребованных товаров.

[99] Одним из самых известных онлайн-форумов по кардингу был DarkMarket, на котором могли удовлетворяться спрос и предложение незаконных материалов, таких как личные и финансовые данные [865–867].

[100] Аналогично тому, как это происходит в реальном мире, где большинству традиционных преступников нужен канал для легитимизации их преступных доходов, киберпреступники также нуждаются в выходе из цифровой финансовой системы. Типичные провайдеры, такие как денежные «мулы», играют заметную роль в соединении онлайн и оффлайн миров [868].

[101] По данным Positive Technologies, во втором квартале 2020 года число кибератак выросло на 59% по сравнению с аналогичным периодом 2019. По данным компании

ж) переход на дистанционную работу, повысивший нагрузку на корпоративную безопасность за счет растущего числа атак на веб-приложения[102] [783];

з) расширение использования технологий биометрии для противодействия киберпреступлениям;

и) увеличение количества атак на IoT, включая такие устройства, как веб-камеры, «умные» часы, телевизоры и пр.[103].

к) масштабная цифровизация предприятий, которая привела к необходимости комплексной защиты критической и промышленной инфраструктуры: медицинских учреждений, производств, финансового сектора, транспортных систем, телекоммуникаций, энергетики, систем водоснабжения и т. д., поскольку данные предприятия оказались в большей степени подвержены киберугрозам [855]. В настоящее время отмечается специализация ряда профессиональных группировок на целевых атаках предприятий в таких секторах, как энергетика, машиностроение и промышленность. Более того, фиксируются кибератаки, нацеленные на автоматизированные системы управления технологическим процессом, промышленные сети, IoT и критическую инфраструктуру в целом.

Следует отметить рост ущерба для экономики от глобальной киберпреступности за 2014–2017 годы с 445 млрд долларов до 608 млрд долларов.

Отчет, опубликованный Symantec, показал, что в 2017 году от киберпреступности пострадали 978 млн человек в 20 странах мира [870] на сумму 172 млрд долларов (в среднем 142 доллара на жертву) для потребителей. Кроме того, эти киберпреступления

«Ростелеком», за первые полгода 2020 года объем киберпреступлений в отношении организаций вырос на 40% по сравнению с аналогичным периодом 2019 года. Согласно данным МВД России, в первом полугодии 2020 года число киберпреступлений выросло на 91,7% на фоне снижения традиционной преступности (Криминал перешел в интернет. – Режим доступа: https://www.kommersant.ru/doc/4544119?tg. – Дата доступа: 23.10.2020).

[102] Среднее ежедневное число атак методом брутфорса – автоматизированного перебора паролей – на базы данных в апреле 2020 года выросло на 23% по сравнению с январем того же года и фишинга на тему пандемии коронавируса (с конца февраля 2020-го количество фишинговых атак по электронной почте увеличилось более чем на 600%).

[103] Рост атак на домашние сети, «умные» устройства и роутеры в первом полугодии 2020 года отмечают в компании Trend Micro (Заокеанские клики. – Режим доступа: https://www.kommersant.ru/doc/4574900?tg. – Дата доступа: 17.11.2020).

не только приносят финансовые потери, но и оказывают психологическое и социальное влияние на благополучие жертв [871].

Анализ отчета о прогнозировании угроз и оценки идентичности Университета Техаса [872, 873] показал, что в 2019 году кражи цифровых данных увеличились на 25% по сравнению с 2018 годом.

Согласно отчету WEF, менее чем за десять лет кибербезопасность стала одной из наиболее важных системных проблем для мировой экономики. Коллективные глобальные расходы достигли 145 млрд долларов в год и, по прогнозам, в ближайшие годы превысят 1 трлн долларов [874]. По оценкам ЕС, издержки от киберпреступлений для мировой экономики к 2020 году превысили 5,5 трлн евро (двухкратный рост с 2015 года), более 12% всех европейских компаний уже были атакованы киберпрестпниками [238]. При этом, несмотря на рекордные расходы на кибербезопасность, по данным ряда исследований, 53% из 3000 опрошенных компаний были плохо подготовлены к противодействию кибератакам [875, 876]. Согласно разным оценкам, средняя утечка данных обходится около 3,7 млн долларов [877, 878]. После того как информация о кибервзломе становится достоянием общественности, средняя цена акций достигает дна и отстает от NASDAQ на –3,5%. Через шесть месяцев средняя динамика цены акций падает на –3,0% по сравнению с динамикой NASDAQ и тем самым снижает капитализацию предприятия [879].

Заключение

Таким образом, риски цифровизации на базовом уровне отраслей и предприятий обусловлены, в том числе, внедрением технологий IoT, BDA, AI, Blockchain, Cloud, а также бизнес-операционных (производственных) систем. Интеграция, специфика и элементные составляющие для концептов «Новой экономики 2.0» различаются, что обусловливает уязвимость их имплементации в реальном секторе.

Проведен сравнительный анализ и выделены ключевые блоки рисков имплементации технологических решений IoT, Cloud, AI, BDA, Блокчейн, включающие кибербезопасность систем, конфиденциальность данных, отсутствие общих стандартов и совместимость. Для ключевых концептов выделены общие и специфические

группы рисков и угроз. Так, для концепций Industry 4.0, Agriculture 4.0, Smart Grid, Smart Supply Chain, E-Commerce и Smart City предполагается формирование оцифрованных сред в форме двух взаимосвязанных сетей: информационной и производственной. Результирующие взаимосвязи в оцифрованных производственных средах создают увеличенную поверхность атаки и больше возможностей для их распространения, включая угрозы безопасности оборудования; наличие сетевых уязвимостей; недостаточность ресурсов для осуществления эффективного контроля безопасности в режиме реального времени на уровне аутентификации, авторизации и шифрования; уязвимость промышленных Big Data в силу значительности их массива, сложности и использования как внутри, так и вовне среды предприятий; отсутствие стандартизации в рамках концепции IoT приведет к нарастанию проблем совместимости, надежности, безопасности и эффективной работы между гетерогенными решениями.

Внедрение облачных технологий в таких секторах, как банковский, телекоммуникаций, производственные предприятия, формирует следующий корпус угроз и рисков: безопасность используемого программного обеспечения; надежность инфраструктуры; обеспечение безопасности хранения цифровых данных; сетевая безопасность; гарантия анонимности данных; обеспечение целостности, конфиденциальности и доступности информации.

В условиях интеграции внутренних сетей управления энергосистемами с внешними сетями возникает вероятность осуществления скоординированных кибератак, которые могут одновременно нацеливаться на достаточное количество критически важного энергогенерирующего оборудования, чтобы вызвать каскадные эффекты и в конечном итоге привести к краху энергосистемы. Электроэнергетика является составной частью критической национальной инфраструктуры, которая определяет стабильность функционирования жизненно важных сфер в контексте, в том числе экономической безопасности государства. Отказ инфраструктуры или недоступность услуг может привести к значительным разрушениям и оказать негативное влияние на промышленное производство, безопасность жизни граждан и имущества.

Цифровизация финансовой инфраструктуры способствует росту уязвимостей и рисков стабильного развития банковской системы, значительное расширение банковских онлайн-операций

послужило причиной роста мошеннических банковских операций в Интернете. Кибератаки в финансовой сфере направлены на перехват и преступное воздействие на сферу банковского управления и контроля посредством кражи и нарушения целостности данных; коммерческого шпионажа; мошенничества.

Реализация концепции Smart City сталкивается с угрозами безопасности со стороны киберпреступников по причине хрупкости системы и широких возможностей для утечки данных. Кибератаки могут быть направлены на каждый компонент Smart City, включая системы диспетчерского управления и сбора данных для мониторинга городской инфраструктуры, датчики и контроллеры IoT. Сети связи могут быть взломаны, в результате чего вызвать сбои в работе всей системы, нарушить целостность обмена информацией и конфиденциальность цифровых данных пользователей. Целостность данных является основной проблемой безопасности, связанной с функционированием интеллектуальной транспортной системы. Преступное изменение цифровых данных в автономных транспортных средствах может привести не только к имущественному ущербу, но и физической угрозе водителей и пешеходов.

Блокчейн интегрируется как в традиционные отрасли на базе концепций Industry 4.0, Smart Grid, Smart Chain Supply и прочих, так и, главным образом, FinTech-идустрию. Среди рисков внедрения данной технологии выделяют плохую защиту криптовалютной индустрии, что создает потенциал для кражи криптовалютных активов пользователей, в особенности с применением специально разработанного вредоносного ПО.

С учетом специфики внедряемых цифровых систем на уровне отраслей сформирована матрица секторальных киберугроз, среди наиболее распространенных и опасных инструментов кибератак выделены вредоносные программы, целевые и DDos-кибератаки. Проведен сравнительный анализ характеристик различных данных киберинструментов с учетом их потенциальной направленности в отношении секторов и сегментов экономики, а также разработана матрица рисков на уровне экономики для различных киберинструментов.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Философский энциклопедический словарь / гл. ред.: Л. Ф. Ильичёв [и др.]. – М.: Сов. энцикл., 1983. – 840 с.

2. Бернар, И. Толковый экономический и финансовый словарь: в 2 т. / И. Бернар, Ж.-К. Колли. – М.: Международные отношения, 1994. – Т 1. – 784 с.

3. Толковый словарь Финам. [Электронный ресурс]. – Режим доступа: https://www.finam.ru/dictionary/wordf0077E00031/?page=1 (дата обращения: 23.03.2022).

4. Narkus, S. A long-waves theory / S. Narkus, N. Kondratieff, J. Schumpeter; Universitetet in OSLO. – 2012. – 80 p. – URL: https://www.duo.uio.no/bitstream/handle/10852/38107/Sarunas-Narkus.pdf?sequence=1 (date of access: 15.02.2021).

5. Beyond the Digital Economy: A Perspective on Innovation for the Learning Society / P. Conceicao [et al.] // Technological Forecasting and Social Change. – 2001. – Vol. 67. – P. 115–142.

6. Кондратьев, Н. Д. Большие циклы конъюнктуры и теория предвидения / Н. Д. Кондратьев, Ю. В. Яковец, Л. И. Абалкин // Избранные труды. Экономика. – М., 2002. – 550 с. – Режим доступа: https://bmstu.ru/ps/~EGavrilina/fileman/download/%D0%A1%D0%BE%D1%86%D0%B8%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D1%8F%20%D0%B8%D0%BD%D0%BD%D0%BE%D0%B2%D0%B0%D1%86%D0%B8%D0%B9/%D0%91%D0%BE%D0%BB%D1%8C%D1%88%D0%B8%D0%B5%20%D1%86%D0%B8%D0%BA%D0%BB%D1%8B%20%D0%BA%D0%BE%D0%BD%D1%8A%D1%8E%D0%BD%D0%BA%D1%82%D1%83%D1%80%D1%8B%D0%9A%D0%BE%D0%BD%D0%B4%D1%80%D0%B0%D1%82%D1%8C%D0%B5%D0%B2.pdf (дата обращения: 14.06.2021).

7. Schumpeter, J. The Theory of Economic Development: An Inquiry Into Profits, Capital, Credit, Interest, and the Business Cycle / J. Schumpeter. – Cambridge, MA: Harvard University Press, 1949. – 250 p. – URL: https://archive.org/details/in.ernet.dli.2015.187354/page/n1/mode/2up (date of access: 20.12.2020).

8. Chen, J. Holistic Innovation: An Emerging Innovation Paradigm / J. Chen, X. Yin, L. Mei // International Journal of Innovation Studies. – 2018. – No. 2. – P. 1–13. – DOI: 10.1016/j.ijis.2018.02.001.

9. Schumpeter, J. A. The theory of economic development / J. A. Schumpeter. – London: Routledge, 1980. – 320 p.

10. Schumpeter, J. A. Capitalism, Socialism and Democracy / J. A. Schumpeter. – London; New-York: Routledge, 2003. – 437 p. – URL: https://periferiaactiva.files.wordpress.com/2015/08/joseph-schumpeter-capitalism-socialism-and-democracy-2006.pdf (date of access: 16.11.2021).

11. Freeman, C. Unemployment and Technical Change / C. Freeman, J. Clark, L. Soete. – London: Frances Pinter, 1982. – 214 p.

12. Wonglimpiyarat, J. S-curve trajectories of electronic money innovations // Journal of High Technology Management Research. – 2016. – Vol. 27. – P. 1–9. – DOI: 10.1016/j.hitech.2016.04.001.

13. Freeman, C. Structural crises of adjustment, business cycles and investment behavior / C. Freeman, C. Perez // Technical Change and Economic Theory / eds.: G. Dosi [et al.]. – London; New-York: Pinter, 1988. – P. 38–66.

14. Nelson, R. An evolutionary theory of economic change / R. Nelson, S. Winter. – Boston, M.A.: Harvard University Press, 1982. – 437 p.

15. Pavitt, K. Strategic management in the innovating firm / K. Pavitt // Frontiers of management / ed. R. Mansfield. – London: Routledge, 1989. – 298 p.

16. Rosenberg, N. Learning by using / N. Rosenberg // Inside the black box: Technology and economics / ed. N. Rosenberg. – Cambridge: Cambridge University Press, 1982. – 304 p.

17. Kuhn, T. S. The structure of scientific revolutions / T. S. Kuhn. – Chicago: University of Chicago Press, 1970. – 210 p.

18. Freeman, C. The economics of industrial innovation / C. Freeman, L. Soete. – London: The M. I. T. Press, 1997. – 470 p. – DOI: 10.4324/9780203357637.

19. Freeman, C. A hard landing for the ‘New Economy’? Information technology and the United States national system of innovation / C. Freeman // Structural Change and Economic Dynamics. – 2001. – No. 12. – P. 115–139.

20. Freeman, C. As Time Goes By: From the Industrial Revolutions to the Information Revolution / C. Freeman, F. Louca. – Oxford: Oxford University Press, 2002. – 432 p.

21. A review of machine learning for new generation smart dispatch in power systems / L. Yin [et al.] // Engineering Applications of Artificial Intelligence. – 2020. – No. 88. – P. 1–12. – DOI: 10.1016/j.engappai.2019.103372.

22. Achieving a Sustainable Shipbuilding Supply Chain under I4.0 perspective / M. Ramirez-Pena [et al.] // Journal of Cleaner Production. – 2020. – Vol. 244. – P. 1–20. – DOI: 10.1016/j.jclepro.2019.118789.

23. Bundesministerium fur Wirtschaft und Energie. Plattform Industrie 4.0. Was ist Ind. 4.0? – 2019. – URL: https://www.plattform-i40.de/I40/Navigation/EN/Home/home.html (date of access: 26.11.19).

24. Veblen, T. The Theory of the Leisure Class / T. Veblen. – N. Y.: Cosimo Classics, 2007. – 256 p.

25. Bush, P. The theory of institutional change / P. Bush // Evolutionary Economics I: Foundations of Institutional Thought / ed. M. R. Tool. – NY: Armonk, 1988. – P. 125–166.

26. Reinecke, J. When times collide: Temporal brokerage at the intersection of markets and developments / J. Reinecke, S. Ansari // Academy of Management Journal. – 2015. – Vol. 58 (2). – P. 618–648.

27. Mansfield, E. The economics of technological change / E. Mansfield. – N.Y.: W.W. Norton & Company Inc., 1968. – 257 p.

28. Mansfield, E. Industrial research and technological innovation: An econometric analysis / E. Mansfield. – N. Y.: W. W. Norton, Yale University, 1968. – 235 p.

29. Crossan, M. A multi-dimensional framework of organizational innovation: A systematic review of the literature / M. Crossan, M. Apaydin // Journal of Management Studies. – 2010. – Vol. 47 (6). – P. 1154–1191.

30. Tushman, M. Technological discontinuities and organization environments / M. Tushman, P. Anderson // Administrative Science Quarterly. – 1986. – Vol. 31, No. 3. – P. 439–465.

31. Abernathy, W. Innovation: Mapping the winds of creative destruction / W. Abernathy, K. Clark // Research Policy. – 1985. – Vol. 14 (1). – P. 3–22.

32. Utterback, J. A dynamic model of process and product innovation / J. Utterback, W. Abernathy // Omega. – 1975. –Vol. 3 (6). – P. 639–656.

33. Vernon, R. International investment and international trade in the product cycle / R. Vernon // Quarterly Journal of Economics. – 1966. – Vol. 80 (2). – P. 190–207.

34. Abernathy, W. Industrial renaissance: Producing a competitive future for America / W. Abernathy, K. Clark, A. Kantrow. – New York: Basic Books Inc., 1983. – 194 p.

35. Christensen, C. Seeing What's Next: Using the Theories of Innovation to Predict Industry Change / C. Christensen, S. Anthony, E. Roth. – Boston, MA: Harvard Business Press, 2004. – 352 p.

36. Новикова, И. В. Системный кризис мировой экономики или кризис системы? / И. В. Новикова // Международный научно-общественный журнал Мир перемен. – 2020. – № 2. – С. 98–109.

37. Nelson, R. National Innovation Systems / R. Nelson. – Oxford: Oxford University Press, 1991. – 560 p.

38. Pavitt, K. Sectoral patterns of technical change: Towards a taxonomy and a theory / K. Pavitt // Research Policy. – 1984. – Vol. 13 (6). – P. 343–374.

39. Tidd, J. Managing innovation: Integrating technological, market and organizational change / J. Tidd, J. Bessant. – Chichester: John Wiley & Sons, 2009. – 638 p.

40. Daft, R. Bureaucratic versus non bureaucratic structure and the process of innovation and change / R. Daft // Research in the Sociology of Organizations. – 1982. – Vol. 1. – P. 129–166.

41. Rothwell, R. Invention, innovation, reinnovation and the role of user / R. Rothwell, P. Gardiner // Technovation. – 1985. – Vol. 3. – P. 168–186.

42. Chesbrough, H. Open services innovation: Rethinking your business to grow and compete in a new era / H. Chesbrough. – San Francisco, CA: Jossey Bass, 2011. – 256 p.

43. Chesbrough, H. When is virtual virtuous? / H. Chesbrough, D. Teece // Harvard Business Review. – 1996. – Vol. 74 (1). – P. 65–73.

44. Wonglimpiyarat, J. The systemness characteristics of financial innovations: Network of electronic payment / J. Wonglimpiyarat // International Journal of Financial Services Management. – 2006. – Vol. 1 (2/3). – P. 255–266.

45. Schuelke-Leech, B.-A. A model for understanding the orders of magnitude of disruptive Technologies / B.-A. Schuelke-Leech // Technological Forecasting & Social Change. – 2017. – Vol. 129. – P. 261–-274. – DOI: 10.1016/j.techfore.2017.09.033.

46. Florida, R. The Break-Through Illusion: Corporate America's Failure to Move From Innovation to Mass Production / R. Florida, M. Kenney. – New York: Basic Books, 1992. – 272 p.

47. Morone, J. Technology and competitive advantage – The role of general management / J. Morone // Research-Technology Management. – 1993. – Vol. 32 (2). – P. 16–25.

48. Utterback, J. Mastering the Dynamics of Innovation / J. Utterback. – Boston, MA: Harvard Business School Press, 1994. – 288 p.

49. Глазьев, С. Ю. Эволюция технико-экономических систем: возможности и границы централизованного регулирования / С. Ю. Глазьев, Д. С. Львов, Г. Г. Фетисов. – М.: Российская академия наук, Центральный экономико-математический институт: Наука, 1992. – 208 с. – Режим доступа: https://www.twirpx.com/file/2146469/grant/ (дата обращения: 07.08.2021).

50. Глазьев, С. Ю. Теория долгосрочного технико-экономического развития / С. Ю. Глазьев. – М.: Владар, 1993. – 310 с. – Режим доступа: https://istina.msu.ru/publications/book/85805295/ (дата обращения: 08.08.2021).

51. Глазьев, С. Ю. Современная теория длинных волн в развитии экономики / С. Ю. Глазьев // Экономическая наука современной России. – 2012. – № 2 (57). – 16 с. – Режим доступа: https://cyberleninka.ru/article/n/sovremennaya-teoriya-dlinnyh-voln-v-razvitii-ekonomiki/viewer (дата обращения: 08.08.2021).

52. Christensen, C. Customer power, strategic investment, and the failure of leading firms / C. Christensen, J. Bower // Strategic Management Journal. – 1996. – Vol. 17 (3). – P. 197–218.

53. Beinhocker, E. The Origin of Wealth: Evolution, Complexity, and the Radical Remaking of Economics / E. Beinhocke. – Boston, MA: Harvard Business School Press, 2006. – 527 p.

54. Kondratieff, N. The Long Waves in Economic Life / N. Kondratieff // Review. – 1979. – Vol. II, No. 4. – P. 519–562.

55. Schumpeter, J. Business Cycles: A Theoretical, Historical, and Statistical Analysis of the Capitalist Process / J. Schumpeter. – NY: McGraw-Hill Book Company Inc., 1939. – 461 p.

56. Paulin, A. Economic Value of Technological Ecosystems / A. Paulin // Smart City Governance. – 2019. – Chapter 11. – P. 203–216. – DOI: 10.1016/B978-0-12-816224-8.00011-X.

57. Bresnahan, T. General purpose technologies: «engines of growth»? / T. Bresnahan, M. Trajtenberg // Journal of Economics. – 1995. – Vol. 65 (1). – P. 83–108.

58. Lipsey, R. Economic Transformations: General Purpose Technologies and Long-Term Economic Growth / R. Lipsey, K. Carlaw, C. Bekar. – Oxford: Oxford University Press, 2006. – 616 p.

59. Jovanovic, B. General purpose technologies / B. Jovanovic, P. Rousseau // Handbook of Economic Growth / eds: P. Aghion, S. N. Durlauf. – Cambridge: Elsevier, 2005. – Vol. 1. – P. 1181–1224.

60. Teece, D. Profiting from innovation in the digital economy: Enabling technologies, standards, and licensing models in the wireless world / D. Teece // Research Policy. – 2018. – Vol. 47 (8). – P. 1367–1387. – DOI: 10.1016/j.respol.2017.01.015.

61. Carlaw, K. Externalities, technological complementarities and sustained economic growth / K. Carlaw, R. Lipsey // Research Policy. – 2002. – Vol. 31 (8). – P. 1305–1315.

62. Guidelines for collecting, reporting and using data on innovation / Oslo Manual 2018 // OECD. – 2018. – 258 p. – URL: https://www.oecd.org/science/oslo-manual-2018-9789264304604-en.htm (date of access: 13.10.2020).

63. Lashitew, A. Mobile phones for financial inclusion: What explains the diffusion of mobile money innovations? / A. Lashitew, R. van Tulder, Y. Liasse // Research Policy. – 2019. – No. 48. – P. 1201–-1215. – DOI: 10.1016/j.respol.2018.12.010.

64. Freeman, C. The 'National System of Innovation' in historical perspective / C. Freeman // Cambridge Journal of Economics. – 1995. – Vol. 19. – P. 5–24.

65. Niosi, J. Technology, development and innovation systems: an introduction / J. Niosi // Journal of Development Studies. – 2008. – Vol. 44 (5). – P. 613–621.

66. Bergek A. Analyzing the functional dynamics of technological innovation systems: a scheme of analysis / A. Bergek [et al.] // Research Policy. – 2008. – Vol. 37. – P. 407–429.

67. Hekkert M. Functions of innovation systems: a new approach for analyzing technological change / M. Hekkert [et al.] // Technological Forecasting and Social Change. – 2007. – Vol. 74. – P. 413–432.

68. The National System of Innovation / ed. B.-A. Lundvall. – London: Pinter, 1992. – 342 p.

69. National Innovation Systems: A Comparative Analysis / ed. R. Nelson. – Oxford: Oxford University Press, 1993. – 541 p.

70. Wonglimpiyarat, J. Challenges and dynamics of FinTech crowdfunding: An innovation system approach / J. Wonglimpiyarat // Journal of High Technology Management Research. – 2018. – Vol. 29 (1). – P. 98–108. – DOI: 10.1016/j.hitech.2018.04.009.

71. Carlsson, B. Internationalization of innovation systems: A survey of the literature / B. Carlsson // Research Policy. – 2006. – Vol. 35 (1). – P. 55–67.

72. Mani, S. Financing of innovation – A survey of various institutional mechanisms in Malaysia and Singapore / S. Mani // Journal of Technology Innovation. – 2004. – Vol. 12 (2). – P. 185–208.

73. Bazavan, A. Chinese government's shifting role in the national innovation system / A. Bazavan // Technological Forecasting & Social Change. – 2019. – Vol. 148. – P. 1–11. – DOI: 10.1016/j.techfore.2019.119738.

74. Li, Y. Innovation Pathways in the Chinese Economy / Y. Li // Georgia Institute of Technology. – 2017. – URL: https://smartech.gatech.edu/handle/1853/59127 (date of access: 22.11.2020).

75. Filippetti, A. Innovation in times of crisis: national systems of innovation, structure, and demand / A. Filippetti, D. Archibugi // Research Policy. – 2011. – Vol. 40 (2). – P. 179–192. – DOI: 10.1016/j.respol.2010.09.001.

76. Fagerberg, J. National innovation systems, capabilities and economic development / J. Fagerberg, M. Srholec // Research Policy. – 2008. – Vol. 37 (9). – P. 1417–1435. – DOI: 10.1016/j.respol.2008.06.003.

77. A technology delivery system for characterizing the supply side of technology emergence: Illustrated for Big Data & Analytics Technological Forecasting & Social Change / Y. Huang [et al.] // Technological Forecasting and Social Change. – 2018. – Vol. 130 (C). – P. 165–176. – DOI: 10.1016Zj.techfore.2017.09.012.

78. Branscomb L. Federal support of commercially relevant R&D / L. Branscomb // American Scientist. – 1973. – Vol. 61. – P. 144–151.

79. Ezra, A. Technology utilization: incentives and solar energy / A. Ezra // Science. – 1975. – Vol. 187. – P. 707–713.

80. Wenk, E. Interinstitutional networks in technological delivery systems / E. Wenk, T. Kuehn // Science and Technology Policy: Perspectives and Developments / ed. J. Haberer. – Massachusetts: Lexington Books, 1977. – P. 153–175.

81. Industrial robots – a strategic forecast using the technological delivery system approach / A. Porter [et al.] // IEEE Transactions on Systems, Man, and Cybernetics. SMC-15. – 1985. – Vol. 4. – P. 521–527.

82. Etzkowitz, H. The dynamics of innovation: from National Systems and “Mode 2” to a triple helix of university-industry-government relations / H. Etzkowitz, L. Leydesdorff // Research Policy. – 2000. – Vol. 29. – P. 109–123.

83. Караянис, Э. Четырехзвенная спираль инноваций и «умная специализация»: производство знаний и национальная конкурентоспособность / Э. Караянис, Э. Григорудис // Форсайт. – 2016. – Т. 10. – № 1. – С. 31–42.

84. Callon, M. Techno-economic networks and irreversibility / M. Callon // The Sociological Review. – 1990. – Vol. 38. – P. 132–161.

85. The management and evaluation of technological programs and the dynamics of techno-economic networks: the case of the AFME / M. Callon [et al.] // Research Policy. – 1992. – Vol. 21. – P. 215–236.

86. Queiroz, M. Blockchain adoption challenges in supply chain: An empirical investigation of the main drivers in India and the USA / M. Queiroz, S. Wamba // International Journal of Information Management. – 2019. – Vol. 46. – P. 70–82.

87. Al-Sayyed, F. Interventional factors affecting instructors adoption of e-learning system: A case study of Palestine / F. Al-Sayyed, B. Abdalhaq // Journal of Theoretical and Applied Information Technology. – 2016. – Vol. 83 (1). – P. 119–137. – DOI: 10.1287/mnsc.46.2.186.11926.

88. Venkatesh, V. Consumer acceptance and user of information technology: Extending the unified theory of acceptance and use of technology / V. Venkatesh, J. Thong, X. Xu // MIS Quarterly. – 2012. – Vol. 36 (1). – P. 157–178. – DOI: 10.1111/j.1365-2729.2006.00163.x.

89. Assessing regional digital competence: Digital futures and strategic planning implications / K. Alam [et al.] // Journal of Rural Studies. – 2018. – Vol. 60. – P. 60–69. – DOI: 10.1016/j.jrurstud.2018.02.009.

90. Davis, F. Technology Acceptance Model for Empirically Testing New End-user Information Systems Theory and Results: Doctoral Dissertation / F. Davis. – Cambridge: MIT, 1986. – 291 p.

91. Tornatzky, G. The Processes of Technological Innovation / G. Tornatzky, M. Fleischer. – Lexington, MA: Lexington Books, 1990. – 298 p.

92. User acceptance of information technology: Toward a unified view / V. Venkatesh [et al.] // MIS Quarterly. – 2003. – Vol. 27 (3). – P. 425–478. – DOI: 10.2307/30036540.

93. Baig, M. Big data adoption: State of the art and research challenges / M. Baig, L. Shuib, E. Yadegaridehkordi // Information Processing and Management. – 2019. – Vol. 56 (6). – DOI: 10.1016/j.ipm.2019.102095.

94. Goodhue, D. Task-technology it and individual performance / D. Goodhue, R. Thompson // MIS Quarterly. – 1995. – Vol. 19 (2). – P. 213–236. – DOI: 10.2307/249689.

95. Big data and predictive analytics for supply chain and organizational performance / A. Gunasekaran [et al.] // Journal of Business Research. – 2017. – Vol. 70 (1). – P. 308–317. – DOI: 10.1016/j.jbusres.2016.08.004.

96. Mobile payment is not all the same: The adoption of mobile payment systems depending on the technology applied / I. de Luna [et al.] // Technological Forecasting & Social Change. – 2019. – Vol. 146. – P. 931–944. – DOI: 10.1016/j.techfore.2018.09.018.

97. Ajzen, I. Understanding Attitudes and Predicting Social Behavior / I. Ajzen, M. Fishbein. – Londres: Prentice Hall International, 1980. – 278 p.

98. Ajzen, I. The theory of planned behavior / I. Ajzen // Organizational Behavior and Human Decision Processes. – 1991. – Vol. 50. – P. 179–211.

99. Sobhanifard, Y. Consumer-based modeling and ranking of the consumption q factors of cryptocurrencies / Y. Sobhanifard, S. Sadatfarizani // Physica A. – 2019. – Vol. 528. (C). – URL: https://www.researchgate.net/publication/333049083_Consumer-based_modeling_and_ranking_of_the_consumption_factors_of_cryptocurrencies (date of access: 15.12.2020). – DOI: 10.1016/j.physa.2019.121263.

100. Papadopoulos, G. Blockchain and Digital Payments: An Institutionalist Analysis of Cryptocurrencies / G. Papadopoulos // Handbook of Digital Currency. – 2015. – P. 153–172.

101. Brown, M. Digitalization of Energy / M. Brown, S. Woodhouse, F. Sioshansi // Consumer, Prosumer, Prosumager. – London: Academic Press, 2019. – Chapter 1. – P. 3–25. – DOI: 10.1016/B978-0-12-816835-6.00001-2.

102. Dufva, T. Grasping the future of the digital society / T. Dufva, M. Dufva // Futures. – 2019. – No. 107. – P. 17–28. – DOI: 10.1016/j.futures.2018.11.001.

103. G20 Digital economy development and cooperation initiative. China, Ministry of Foreign Affairs of Japan. – 2016. – 8 p. – URL: https://www.mofa.go.jp/files/000185874.pdf (date of access: 23.11.2020).

104. Ruan, K. Principles of Cybernomics. Digital Asset Valuation and Cyber Risk Measurement / K. Ruan. – Cambridge: Elsevier Inc., 2019. – P. 141–158. – DOI: 10.1016/B978-0-12-812158-0.00009-0.

105. Warner, K. Building dynamic capabilities for digital transformation: An ongoing process of strategic renewal / K. Warner, M. Wager // Long Range Planning. – 2019. – Vol. 52 (3). – P. 326–349. – DOI: 10.1016/j.lrp.2018.12.001.

106. Digital affordances, spatial affordances, and the genesis of entrepreneurial ecosystems / E. Autio [et al.] // Strategic Entrepreneurship Journal. – 2018. – Vol. 12 (1). – P. 72–95.

107. Tilson, D. Research commentary - digital infrastructures: the missing IS research agenda / D. Tilson, K. Lyytinen, C. Sorensen // Information Systems Research. – 2010. – Vol. 21 (4). – P. 748–759.

108. Миллер, Я. В. Создание добавленной стоимости в контексте сложности измерения цифровой экономики / Я. В. Миллер // E-Management. – 2020. – Т. 3 – № 1. – С. 68–74. – DOI: 10.26425/2658-3445-2020-1-68-74.

109. OECD. Going Digital: Shaping Policies, Improving Lives / OECD Publishing. – Paris, 2019. – 168 p. – URL: https://read.oecd.org/10.1787/9789264312012-en?format=pdf (date of access: 03.10.2020).

110. Digital transformation: A multidisciplinary reflection and research agenda / P. Verhoef [et al.] // Journal of Business Research. – 2019. – Vol. 122 (C). – P. 889–901. – DOI: 10.1016/jjbusres.2019.09.022.

111. Yoo, Y. Computing in everyday life: a call for research on experiential computing / Y. Yoo // MIS Quarterly. – 2010. – Vol. 34 (2). – P. 213–231. – DOI: 10.2307/20721425.

112. Berry, D. The philosophy of software / D. Berry. – NY: Palgrave Macmillan, 2011. – 211 p. – DOI: 10.1057/9780230306479.

113. Elia, G. Digital entrepreneurship ecosystem: How digital technologies and collective intelligence are reshaping the entrepreneurial process / G. Elia, A. Margherita, G. Passiante // Technological Forecasting & Social Change. – 2020. – Vol. 150 (C). – DOI: 10.1016/j.techfore.2019.119791.

114. European Commission. Digital Transformation Scoreboard. – 2017. – URL: https://ec.europa.eu/growth/tools-databases/dem/monitor/scoreboard (date of access: 01.09.2020).

115. Brynjolfsson, E. The Second Machine Age: Work, вProgress, and Prosperity in a Time of Brilliant Technologies / E. Brynjolfsson, A. McAfee. – New York: Norton and Company, 2014. – 281 p. – URL: https://edisciplinas.usp.br/pluginfile.php/4312922/mod_resource/content/2/Erik%20-%20The%20Second%20Machine%20Age.pdf (date of access: 03.07.2020).

116. Tapscott, D. The Digital Economy Anniversary Edition: Rethinking Promise and Peril in the Age of Networked Intelligence / D. Tapscott. – N.Y: McGraw Hill Professional, 2014. – 448 p.

117. Embracing digital technology: a new strategic imperative / M. Fitzgerald [et al.] // MIT Sloan Management Review. – 2014. – Vol. 55 (2). – P. 1–12.

118. Liu, D.-Y. Resource fit in digital transformation / D.-Y. Liu, S.-W. Chen, T.-C. Chou // Management Decision. – 2011. – Vol. 49 (10). – P. 1728–1742.

119. Rogers, D. The Digital Transformation Playbook: Rethink Your Business for the Digital Age / D. Rogers. – New York: Columbia University Press, 2016. – 296 p.

120. Options for formulating a digital transformation strategy / T. Hess [et al.] // MIS Quarterly Executive. – 2016. – Vol. 15 (2). – P. 123–139. – URL: https://www.researchgate.net/publication/291349362_Options_for_Formulating_a_Digital_Transformation_Strategy (date of access: 14.02.2020).

121. Hinings, B. Digital innovation and transformation: An institutional perspective / B. Hinings, T. Gegenhuber, R. Greenwood // Information and Organization. – 2018. – Vol. 28 (1). – P. 52–61. – DOI: 10.1016/j.infoandorg.2018.02.004.

122. Al-Ruithe, M. Key Issues for Embracing the Cloud Computing to Adopt a Digital Transformation: A study of Saudi Public Sector / M. Al-Ruithe, E. Benkhelifa, K. Hameed // The 9th International Conference on Ambient Systems, Networks and Tuchnologius (ANT 2018) // Procedia Computer Science. – 2018. – Vol. 130. – P. 1037–1043. – DOI: 10.1016/j.procs.2018.04.145.

123. Nieminen, J. Understanding & Managing Digital Transformation - A case study of a large Nordic retailer / J. Nieminen. – 2014. – 104 p. – URL: https://pdfroom.com/books/understanding-managing-digital-transformation-a-case-study-of-a-large-nordic-retailer/E315v6xP5Yy (date of access: 10.01.2020).

124. IDC. Digital Transformation (DX): An Opportunity and an Imperative. – 2015. – URL: https://www.idc.com/prodserv/decisionscapes/RESOURCES/ATTACHMENTS/IDC_254721_ExecBrief_Digital_Transformation.pdf (date of access: 12.12.2020).

125. Положихина, М. А. Регулирование процесса цифровизации экономики: европейский и российский опыт / М. А. Положихина // Россия и мир в XXI веке. – 2018. – № 4. – С. 64–81. – Режим доступа: https://cyberleninka.ru/article/n/regulirovanie-protsessa-tsifrovizatsii-ekonomiki-evropeyskiy-i-rossiyskiy-opyt (дата обращения: 14.03.2020).

126. Доклад о мировом развитии. Цифровые дивиденды: обзор. – Вашингтон: Всемирный банк, 2016. – 58 с. – Режим доступа: https://openknowledge.worldbank.org/bitstream/handle/10986/23347/210671RuSum.pdf (дата обращения: 01.01.2020).

127. Digital business strategy: toward a next generation of insights / A. Bharadwja [et al.] // MIS Quarterly. – 2013. – Vol. 37 (2). – P. 471–482.

128. Goldfarb, A. Digital Economics / A. Goldfarb, C. Tucker // National Bureau of Economic Research. Working Paper. – 2017. – No. 23684. – 89 p. – URL: http://www.nber.org/papers/w23684 (date of access: 14.03.2020).

129. Pramanik, H. Essence of digital transformation – Manifestations at large financial institutions from North America / H. Pramanik, M. Kirtania, A. Pani // Future Generation Computer Systems. – 2019. – Vol. 95 (4.) – P. 323–343. – DOI: 10.1016/j.future.2018.12.003.

130. Mithas, S. How a firm's competitive environment and digital strategic posture influence digital business strategy / S. Mithas, A. Tafti, W. Mitchell // Management Information Systems Quarterly. – 2013. – Vol. 37 (2). – P. 511–536.

131. Lyytinen, K. Digital product innovation within four classes of innovation networks / K. Lyytinen, Y. Yoo, R. Boland // Information Systems Journal. – 2016. – Vol. 26 (1). – P. 47–75.

132. Tiwana, A. Platform evolution: Coevolution of platform architecture, governance, and environmental dynamics / A. Tiwana, B. Konsynski, A. Bush // Information Systems Research. – 2010. – Vol. 21 (4). – P. 675–687.

133. Aldrich, H. The democratization of entrepreneurship? Hackers, Makerspaces, and Crowdfunding / H. Aldrich // Presentation for Academy of Management Annual Meeting. – Philadelphia, 2014. – 7 p. – URL: https://www.researchgate.net/profile/Howard-Aldrich/publication/268520673_The_Democratization_of_Entrepreneurship_Hackers_Makerspaces_and_Crowdfunding/links/546f54730cf216f8cfa9d6c3/The-Democratization-of-Entrepreneurship-Hackers-Makerspaces-and-Crowdfunding.pdf (date of access: 15.04.2020).

134. Ekbia, H. Digital artifacts as quasi-objects: qualification, mediation, and materiality / H. Ekbia // Journal of the Association for Information Science and Technology. – 2009. – Vol. 60 (12). – P. 2554–2566.

135. Kuester, S. Get the show on the road: go-to-market strategies for e-innovations of start-ups / S. Kuester, E. Konya-Baumbach, M. Schuhmacher // Journal of Business Research. – 2018. – Vol. 83. – P. 65–81.

136. Nambisan, S. Digital entrepreneurship: toward a digital technology perspective of entrepreneurship / S. Nambisan // Entrepreneur. Theory. Practice. –2016. – Vol. 41 (6). – P. 1029–1055. – DOI: 10.1111/etap.12254.

137. Botzem, S. Standardization cycles: A process perspective on the formation and discusion of transnational standards / S. Botzem, L. Dobusch // Organization Studies. – 2012. – Vol. 33 (5–6). – P. 737–762.

138. Gawer, A. Industry platforms and ecosystems innovation / A. Gawer, M. Cusumano // Journal of Product Management. – 2013. – Vol. 31 (3). – P. 417–433.

139. Tapscott, D. Blockchain revolution: How the technology behind Bitcoin is changing money, business, and the world / D. Tapscott, A. Tapscott. – NY: Penguin Random House, 2017. – 432 p. – URL: https://itig-iraq.iq/wp-content/uploads/2019/05/Blockchain_Revolution.pdf (date of access: 13.04.2020).

140. Digital innovation management: reinventing innovation management research in a digital world / S. Nambisan [et al.] // Management Information Systems Quarterly. – 2017. – Vol. 41 (1). – P. 223–238.

141. Berente, N. Institutional contradictions and loose coupling: Postimplementation of NASA's enterprise information system / N. Berente, Y. Yoo // Information Systems Research. – 2012. – Vol. 23. – P. 376–396.

142. Davis, G. Politics & society after the corporation / G. Davis // Politics & Society. – 2013. – Vol. 41 (2). – P. 283–308.

143. Majchrzak, A. Technology accordances and constraints in management information systems (MIS): Encyclopedia of Management Theory / A. Majchrzak, M. Markus. – 2012. – 943 p. – URL: http://dspace.vnbrims.org:13000/jspui/bitstream/123456789/4364/1/Encyclopedia%20of%20Management%20Theory.pdf (date of access: 10.04.2020).

144. Moody, D. Measuring the Value of Information: An Asset Valuation Approach / D. Moody, P. Walsh // European Conference on Information Systems (ECIS'99). – URL: http://si.deis.unical.it/zumpano/2004-2005/PSI/lezione2/ValueOfInformation.pdf (date of access: 11.01.2020).

145. How does IT ambidexterity impact organizational agility? / O. Lee [et al.] // Information Systems Research. – 2015. – Vol. 26 (2). – P. 398–417.

146. Eggers, J. Incumbent adaptation to technological change: The past, present, and future of research on heterogeneous incumbent response / J. Eggers, K. Park // Academy of Management Annals. – 2018. – Vol. 12 (1). – P. 357–389.

147. Ragnedda, M. Conceptualizing digital capital / M. Ragnedda // Telematics and Informatics. – 2018. – Vol. 35. – P. 2366–2375. – DOI: 10.1016/j.tele.2018.10.006.

148. Bourdieu, P. An Invitation to Reflexive Sociology / P. Bourdieu, L. Wacquant. – Chicago: The University of Chicago Press, 1992. – 348 p.

149. European Commission, 2015. Digital Transformation of European Industry and Enterprises. – URL: http://ec.europa.eu/DocsRoom/documents/9462/attachments/1/translations/en/renditions/native (date of access: 16.02.2020).

150. Zhao, F. Digital Entrepreneurship: Research and Practice / F. Zhao, A. Collier // 9 Annual Conference of the EuroMed Academy of Business, Sept. 14–16. – Warsaw, Poland, 2016. – P. 2154–2163. – URL: https://emrbi.org/wp-content/uploads/2016/08/euromed2016bof.pdf (date of access: 18.02.2020).

151. Shen, K. Digital entrepreneurship / K. Shen, V. Lindsay, Y. Xu // Information Systems Journal. – 2018. – Vol. 28 (6). – P. 1125–1128.

152. Cyber entrepreneurship: anote on indigenous perspective from adeveloping country / M. Shabbir [et al.] // Social Sciences. – 2016. – Vol. 11 (5). – P. 704–709.

153. Guthrie, C. The digital factory: a hands-on learning project digital entrepreneurship / C. Guthrie // Journal of Entrepreneurship Education. – 2014. Vol. 17 (1). – P. 115–133.

154. Hosu, I. Digital Entrepreneurship and Global Innovation / I. Hosu, I. Iancu. – Pennsylvania: IGI Global, 2016. – 301 p.

155. Standing, C. Fake it until you make it: business model conceptualization in digital entrepreneurship / C. Standing, J. Mattsson // Journal of Strategic Marketing. – 2018. – Vol. 26 (5). – P. 385–399.

156. Davidson, E. Digital entrepreneurship and its sociomaterial enactment / E. Davidson, E. Vaast // IEEE System Sciences (HICSS): 43rd Hawaii International Conference. Jan. 5–8. – Koloa, Hawaii, 2010. – P. 1–10.

157. Watanabe, X. A new paradox of the digital economy - Structural sources of the limitation of GDP statistics / X. Watanabe, Y. Tou, P. Neittaanmäki // Technology in Society. – 2018. – Vol. 55 (C). – P. 9–23. – DOI: 10.1016/j.techsoc.2018.05.004.

158. Tapscott, D. Governance in the Digital Economy / D. Tapscott, D. Agnew // Issues for the New Millennium. Finance & Development. – 1999. – P. 34–37. – URL: https://www.imf.org/external/pubs/ft/fandd/1999/12/pdf/tapscott.pdf (date of access: 14.05.2020).

159. Overby, H. Digital Economics / H. Overby, J. Audestad. – 2018. – 262 p. – URL: https://www.researchgate.net/profile/Harald-Overby/publication/341312807_Digital_Economics_How_Information_and_Communication_Technology_is_Shaping_Markets_Businesses_and_Innovation/links/5eba605392851cd50dab64aa/Digital-Economics-How-Information-and-Communication-Technology-is-Shaping-Markets-Businesses-and-Innovation.pdf (date of access: 14.05.2020).

160. Бухт, Р. Определение, концепция и измерение цифровой экономики / Р. Бухт, Р. Хикс // Вестник международных организаций. – 2018. – Т. 13, № 2. – С. 143–172 – DOI: 10.17323/1996-7845-2018-02-07.

161. OECD. Measuring ICT Usage and Electronic Commerce in Enterprises: Proposal for a Model Questionnaire. – Paris: OECD, 2001. – P. 1–16.

162. Measuring the Digital Economy. – Washington: IMF, 2018. – URL: https://www.imf.org/~/media/Files/Publications/PP/2018/022818 MeasuringDigitalEconomy. ashx (date of access: 12.01.2020).

163. Четвертая промышленная революция. Популярно о главных технологических трендах XXI в. // Tadviser [Электронный ресурс]. Государство. Бизнес. ИТ. – 17.10.2017. – Электронное обращение: http://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F%3A%D0%A7%D0%B5%D1%82%D0%B2%D0%B5%D1%80%D1%82%D0%B0%D1%8F_%D0%BF%D1%80%D0%BE%D0%BC%D1%8B%D1%88%D0%BB%D0%B5%D0%BD%D0%BD%D0%B0%D1%8F_%D1%80%D0%B5%D0%B2%D0%BE%D0%BB%D1%8 E%D1%86%D0%B8%D1%8F_%28 Industry_4.0%29 (дата обращения: 14.08.2021).

164. Криштаносов, В. Б. Цифровая экономика: современные направления, динамика развития, вызовы / В. Б. Криштаносов // Труды БГТУ. Сер. 5, Экономика и управление. – 2020. – № 1. – С. 13–30.

165. Shapiro, C. Information rules: A strategic guide to the network economy / C. Shapiro, H. Varian. – Harvard: Harvard Business Press, 1998. – 368 p.

166. Ellison, G. Lessons about markets from the internet / G. Ellison, S. Ellison // Journal of Economic Perspectives. – 2005. – Vol. 19 (2). – P.139–158.

167. Bauer, J. Platforms, systems competition, and innovation: Reassessing the foundations of communications policy / J. Bauer // Telecommunications Policy. – 2014. – Vol. 38. – P. 662–673. – DOI: 10.1016/j.telpol.2014.04.008.

168. Whitt, R. Adaptive policymaking: Evolving and applying emergent solutions for U.S. communications policy / R. Whitt // Federal Communications Law Journal. – 2007. – Vol. 61. – P. 483–589.

169. Li, W. Digital entrepreneurship ecosystem as a new form of organizing: the case of Zhongguancun / W. Li, W. Du, J. Yin // Frontiers of Business Research in China. – 2017. – Vol. 11 (1). – P. 69–100. – DOI: 10.1186/s11782-017-0004-8.

170. Dini, P. The (im)possibility of interdisciplinary lessons from constructing a theoretical framework for digital ecosystems / P. Dini, M. Iqani, R. Mansell // Culture, Theory and Critique. – 2011. – Vol. 52 (1). – P. 3–27.

171. Новикова, И. В. Формирование экосистемы цифровой экономики: технологический и институциональный аспекты, международный опыт и имплементация в Республике Беларусь / И. В. Новикова, В. Б. Криштаносов // Белорусский экономический журнал. – 2021. – № 4. – С. 124–137.

172. Ceruzzi, P. A History of Modern Computing / P. A. Ceruzzi. – Massachusets: MIT Press, 2003. – 460 p. – URL: https://doc.lagout.org/science/0_Computer%20Science/0_Computer%20History/A%20History%20of%20Modern%20Computing,%202nd.pdf (date of access: 13.01.2020).

173. Greenstein, S. How the Internet Became Commercial / S. Greenstein. – Princeton: Princeton University Press, 2015. – 488 p.

174. Goldfarb, A. The (teaching) role of universities in the diffusion of the internet / A. Goldfarb // International Journal of Industrial Organization. – 2006. – Vol. 24 (2). – P. 203–225.

175. Internet of Things: Evolution and technologies from a security perspective / R. Ande [et al.] // Sustainable Cities and Society. – 2020. – Vol. 54. – 15 p. – DOI: 10.1016/j.scs.2019.101728.

176. Disrupting Finance. FinTech and Strategy in the 21st Century / ed. Theo Lynn [et al.]. – London: Palgrave Macmillan, 2018. – 175 p.

177. Megargel, A. Real-Time Inbound Marketing: A Use Case for Digital Banking: Handbook of Blockchain / A. Megargel, V. Shankararaman, S. Reddy // Digital Finance, and Inclusion. – 2018. – Vol. 1. – P. 311–327. – DOI: 10.1016/B978-0-12-810441-5.00013-0.

178. Dula, C. Reshaping the Financial Order: Handbook of Blockchain / C. Dula, D. Lee, K. Chuen // Digital Finance, and Inclusion. – 2018. – Vol. 1. – P. 2–18. – DOI: 10.1016/B978-0-12-810441-5.00001-4.

179. Phygital report 2021 // LETA Capital и Devar. – 2021. – URL: https://en.leta.vc/phygital/STATE_OF_PHYGITAL21.pdf (date of access: 11.11.2021).

180. Moscovici, P. Keynote speech at the Masters of Digital 2018 event / P. Moscovici. – Brussels. – 2018. – 3 p.

181. The future of work after COVID 19. The postpandemic economy. – New York: McKinsey Global Institute, 2021. – 152 p. – URL: https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Future%20of%20Organizations/The%20future%20of%20work%20after%20COVID%2019/MGI_The%20Future%20of%20Work%20after%20COVID-19_Report-F.pdf?shouldIndex=false (date of access: 08.02.2022).

182. The Global Risks Report / WEF. – 2021. – 97 p. – URL: http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf (date of access: 09.02.2022).

183. Lemstra, W. Leadership with 5G in Europe: Two contrasting images of the future, with policy and regulatory implications / W. Lemstra // Telecommunications Policy. – 2018. – Vol. 42 (8). – P. 587–611. – DOI: 10.1016/j.telpol.2018.02.003.

184. The 5G business potential. Ericsson. – Stockholm: Ericsson AB, 2017. – 10 p. – URL: https://www.terminsstarttelekom.se/upload/termin/pdf/pres475.pdf (date of access: 21.02.2020).

185. Origins and IoT Landscape / V. Tsiatsis [et al.] // Internet of Things. Technologies and Applications for a New Age of Intelligence. – Cambridge: Elsevier Ltd, 2019. – Chapter 2. – P. 9–30. – DOI: 10.1016/B978-0-12-814435-0.00013-4.

186. Andrade, R. Cognitive security: A comprehensive study of cognitive science in cybersecurity / R. Andrade, S. Yoo // Journal of Information Security and Applications. – 2019. – No. 48. – 13 p. – DOI: 10.1016/j.jisa.2019.06.008.

187. United Nations. Sustainable Developments Goals, 2016. – URL: http://www.undp.org/content (date of access: 28.04.2020).

188. ITU, 2016. Connect 2020 Agenda. – URL: https://www.itu.int (date of access: 15.04.2020).

189. Goudar, S. I. 5G: the next wave of digital society challenges and current trends / S. I. Goudar, S. Hassan, A. Habbal // Journal of Telecommunication, Electronic and Computer Engineering. – 2017. – Vol. 9. – P. 63–66.

190. Gandotra, P. A survey on green communication and security challenges in 5g wireless communication networks / P. Gandotra, R. K. Jha // Journal of Network and Computer Applications. – 2017. – Vol. 96. – P. 39–61.

191. The 5G era: New horizons for advanced-electronics and industrial companies: McKinsey Report / O. Burkacky [et al.]. – February 21, 2020. – 24 p. – URL: https://www.mckinsey.com/~/media/McKinsey/Industries/Advanced%20Electronics/Our%20Insights/The%205G%20era%20New%20horizons%20for%20advanced%20electronics%20and%20industrial%20companies/The-5G-era-New-horizons-for-advanced-electronics-and-industrial-companies.pdf (date of access: 02.06.2021).

192. Gruber, H. Proposals for a digital industrial policy for Europe / H. Gruber // Telecommunications Policy. – 2019. – Vol. 43, issue 2. – P. 116–127. – DOI: 10.1016/j.telpol.2018.06.003.

193. Adib, H. A Context-aware Radio Access Technology selection mechanism in 5G mobile network for smart city applications / H. Adib, I. Swetha, H. Suhaidi // Journal of Network and Computer Applications. – 2019. – Vol. 135. – P. 97–107.

194. Drivers for 5G / S. Rommer [et al.] // 5G Core Networks. Powering Digitalization. – Cambridge: Elsevier Ltd, 2020. – Chapter 2. – P. 7–13. – DOI: 10.1016/B978-0-08-103009-7.00002-8.

195. Ericsson Mobility Report / Ericsson. com. – June 2021. – 36 p. – URL: https://www.ericsson.com/49e50d/assets/local/mobility-report/documents/2021/june-2021-ericsson-mobility-report.pdf (date of access: 03.03.2022).

196. Khajeh-Hosseini, A. Research Challenges for Enterprise Cloud Computing / A. Khajeh-Hosseini, I. Sommerville, I. Sriram. – 2010. – URL: https://www.researchgate.net/publication/45896125_Research_Challenges_for_Enterprise_Cloud_Computing (date of access 09.07.2019).

197. Mell, P. The NIST Definition of Cloud Computing: Version 15, 10.07.2009 / P. Mell, T. Grance. – URL: https://www.nist.gov/system/files/documents/itl/cloud/cloud-def-v15.pdf (date of access: 04.05.2019).

198. Alruwaili, F. Secure migration to compliant cloud services: A case study / F. Alruwaili, A. Gulliver // Journal of Information Security and Applications. – 2018. – Vol. 38. – P. 50–64. – DOI: 10.1016/j.jisa.2017.11.004.

199. Qin, W. Recent advances in industrial internet: Insights and challenges / W. Qin, S. Chen, M. Peng // Digital Communications and Networks. – 2020. – Vol. 6 (1). – P. 1–13. – DOI: 10.1016/j.dcan.2019.07.001.

200. Varian, H. Artificial intelligence, economics, and industrial organization: National Bureau of Economic Research. Working Paper No. 24839 / H. Varian. – July 2018. – 24 p. – URL: http://www.nber.org/papers/w24839 (date of access: 15.04.2019).

201. Sivasakthi, M. Cloud Computing: Introduction and Research Perspective / M. Sivasakthi, M. Jeyakumar // Procedia Computer Science. – 2015. – Vol. 130. – P. 1364–1367.

202. Mazhar, A. Security in cloud computing: Opportunities and challenges / A. Mazhar, K. Samee, A. Vasilakos // Information Sciences. – 2015. – Vol. 305. – P. 357–383.

203. Singh, S. A Survey on Cloud Computing Security: Issues, Threats, and Solutions / S. Singh, Y.-S. Jeong, J. Park // Journal o Network and Computer Applications. – 2016. – Vol. 75. – P. 200–222. – DOI: 10.1016/j.jnca.2016.09.002.

204. Blockchain for cloud exchange: A survey / S. Xie [et al.] // Computers and Electrical Engineering. – 2020. – Vol. 81. – 12 p. – URL: https://www.henrylab.net/wp-content/uploads/2019/12/1-s2.0-S0045790618332750-main.pdf. DOI: 10.1016/j.compeleceng.2019.106526 (date of access: 25.10.2021).

205. Digitalization and Productivity: In Search of the Holy Grail – Firm-level Empirical Evidence from European Countries: OECD Economics Department Working Papers No. 1533. – 2019. – 63 p. – URL: https://www.oecd-ilibrary.org/docserver/5080f4b6-en.pdf?expires=1652693547&id=id&accname=guest&checksum=15FB7E70A9A276B5BD72E1284603B018 (date of access: 14.02.2020).

206. A review of edge computing reference architectures and a new global edge proposal / I. Sittón-Candanedo [et al.] // Future Generation Computer Systems. – 2019. – Vol. 99. – P. 278–294.

207. On multi-access Edge computing: A survey of the emerging 5G network Edge Cloud architecture and orchestration / T. Taleb [et al.] // IEEE Communications Surveys & Tutorials. – 2017. – Vol. 19 (3). – P. 1657–1681. – DOI: 10.1109/COMST.2017.2705720.

208. Cloudsim: A toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms / R. Calheiros [et al.] // Software: Practice and Experience. – 2011. – Vol. 41 (1). – P. 23–50.

209. Osmotic computing: A new paradigm for edge/cloud integration / M. Villari [et al.] // IEEE Cloud Computing. – 2016. – Vol. 3 (6). – P. 76–83.

210. Fog computing and its role in the internet of things / F. Bonomi [et al.] // Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing – MCC ’12. – 2012. –13 p.

211. Edge computing: A survey / Khan W. [et al.] // Future Generation Computer Systems. – 2019. – No. 97. – P. 219–235. – DOI: 10.1016/j.future.2019.02.050.

212. Cisco fog computing solutions: Unleash the power of the Internet of Things. – URL: https://www.cisco.com/c/dam/en_us/solutions/trends/iot/docs/computing-solutions.pdf (date of access: 10.03.2020).

213. Sherlekar, R. Provisioned Data Distribution for Intelligent Manufacturing via Fog Computing / R. Sherlekar, B. Starly, P. Cohen // Procedia Manufacturing. – 2019. – Vol. 34. – P. 893–902. – DOI: 10.1016/j.promfg.2019.06.158.

214. A cloud-edge based data security architecture for sharing and analysing cyber threat information / D. Chadwick [et al.] // Future Generation Computer Systems. – 2020. – No. 102. – P. 710–722.

215. Data security and privacy preserving in edge computing paradigm: Survey and open issues / J. Zhang [et al.] // IEEE Access. – 2018. – Vol. 6. – P. 18209–18237.

216. A novel trust mechanism based on Fog Computing in sensor-cloud system / T. Wang [et al.] // Future Generation Computer Systems. – 2018. – Vol. 109. – P. 573–582. – DOI: 10.1016/j.future.2018.05.049.

217. GAO. Internet of Things. Enhanced assessments and guidance are needed to address security risks. DOD United States Government Accountability Office: Report to Congressional Committees. GAO-17-668. – July 2017. – URL: https://www.gao.gov/assets/690/686203.pdf (date of access: 17.08.2020).

218. GAO. Technology assessment: Internet of things. status and implications of an increasingly connected world. United States Government Accountability Office. Center for Science, Technology, and Engineering: Report to Congressional Requesters. GAO-17-75. – May 2017. – URL: http://www.gao.gov/assets/690/684590.pdf (date of access: 17.08.2020).

219. Kumar, N. Blockchain technology for security issues and challenges in IoT / N. Kumar, P. Mallick // Procedia Computer Science. – 2018. – No. 132. – P. 1815–1823. – DOI: 10.1016/j.procs.2018.05.140.

220. A novel code data dissemination scheme for Internet of Things through mobile vehicle of smart cities / H. Teng [et al.] // Future Generation Computer Systems. – 2019. – Vol. 94. – P. 351–367.

221. Chatfield, A. A framework for Internet of Things-enabled smart government: A case of IoT cybersecurity policies and use cases in U.S. federal government / A. Chatfield, C. Reddick // Government

Information Quarterly. – 2018. – No. 36 (2). – P. 1–12. – DOI: 10.1016/j.giq.2018.09.007.

222. Chatfield, A. Smart city implementation through shared vision of social innovation for environmental sustainability: A case study of Kitakyushu, Japan / A. Chatfield, C. Reddick // Social Science Computer Review. – 2016. – Vol. 34 (6) – P. 757–773.

223. Latta, B. Internet of things working group year-end white paper / B. Latta, P. Welch. – 2016. – URL: https://latta.house.gov/uploadedfiles/iot_working_group_white_paper.pdf (date of access: 17.09.2020).

224. Castro, D. How is the federal government using the Internet of things? Center for Data Innovation / D. Castro, J. New, A. McQuinn. – 2016. – URL: http://www2.datainnovation.org/2016-federal-iot.pdf (date of access: 14.08.2019).

225. Dib, O. A novel data exploitation framework based on Blockchain / O. Dib, C. Huyart, K. Toumi // Pervasive and Mobile Computing. – 2020. – Vol. 61. – 33 p. – DOI: 10.1016/j.pmcj.2019.101104.

226. Internet of things: A survey on enabling technologies, protocols, and applications / A. Al-Fuqaha [et al.] // IEEE Communications Surveys & Tutorials. – 2015. – Vol. 17 (4). – P. 2347–2376.

227. Modeling the internet of things adoption barriers in food retail supply chains / S. Kamble [et al.] // Journal of Retailing and Consumer Services. – 2019. – Vol. 48. – P. 154–168. – DOI: 10.1016/jjretconser.2019.02.020.

228. Vision, applications and future challenges of Internet of Things: a bibliometric study of the recent literature / D. Mishra [et al.] // Industrial Management & Data Systems. – 2016. – Vol. 116 (7). – P. 1331–1355.

229. A review of essential standards and patent landscapes for the Internet of Things: a key enabler for Industry 4.0 / A. Trappey [et al.] // Advanced Engineering Informatics. – 2017. – Vol. 33. – P. 208–229.

230. Challenges in supply chain redesign for the Circular Economy: a literature review and a multiple case study / G. Bressanelli, M. Perona, N. Saccani // International Journal of Production Research. – 2018. – Vol. 57 (23). – P. 7395–7422. – DOI: 10.1080/00207543.2018.1542176.

231. Insurers Need to Plug into the Internet of Things – or Risk Falling Behind: McKinsey report / M. Loffler [et al.]. – 2016. – 11 p. – URL: https://www.mckinsey.com/~/media/McKinsey/Industries/Financial%20Services/Our%20Insights/European%20insurance%20practice%20report%20on%20Internet%20of%20Things/McKinsey%20-%20Insurers%

20need%20to%20plug%20into%20the%20Internet%20of%20Things%20or%20risk%20falling%20behind.pdf (date of access: 09.01.2020).

232. Rad, B. Internet of Things: trends, opportunities, and challenges / B. Rad, H. Ahmada // International Journal of Computer Science and Network Security. – 2017. – Vol. 17 (7). – P. 89–95. – URL: https://www.researchgate.net/publication/326919200_Internet_of_Things_Trends_Opportunities_and_Challenges (date of access: 14.03.2019).

233. Intel. Intel security's international internet of things smart home survey shows many respondents sharing personal data for money. – 2016. – URL: https:// newsroom.intel.com/news-releases/intel-securitys-international-internet-of-things-smart-home-survey/ (date of access: 02.11.2019).

234. Statista. Press Releases. – 2017. – URL: https://www.statista.com (date of access: 05.07.2020).

235. Internet of Things (IoT) Market: Global demand, Growth Analysis&Opportunity Outlook 2023: Nester Research. – 2018. – URL: https://www.researchnester.com/reports/internet-of-things-iot-market/1189 (date of access: 02.01.2019).

236. The Internet of Things: Mapping the value beyond the hype / McKinsey. – 2015. – URL: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/The%20Internet%20of%20Things%20The%20value%20of%20digitizing%20the%20physical%20world/Unlocking_the_potential_of_the_Internet_of_Things_Executive_summary.ashx? (date of access: 23.11.2018).

237. Evans, D. The Internet of Things: How the next evolution of the internet is changing everything / D. Evans // CISCO White Paper. – No. 1. – 2011. – P. 1–11.

238. The EU's Cybersecurity Strategy in the Digital Decade: European Comission. – 2020. – URL: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade (date of access: 03.04.2021).

239. Chui, M. The Internet of Things: Catching up to an accelerating opportunity: Special Report / M. Chui, M. Collins, M. Patel // McKinsey & Company. – 2021. – 90 p. – URL: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/iot-value-set-to-accelerate-through-2030-where-and-how-to-capture-it#download/%2F~%2Fmedia%2Fmckinsey%2Fbusiness%20functions%2Fmckinsey%20digital%2Four%20insights%2Fiot%20value%20set%20to%20accelerate%20through%202030%20where%20and%20how%20to%20capture%20it%2Fthe-internet-of-things-catching-up-to-an-accelerating-opportunity-final.pdf (date of access: 06.12.2021).

240. Moreno, M. User-centric smart buildings for energy sustainable smart cities / M. Moreno, M. Zamora, A. Skarmeta // Transactions on Emerging Telecommunications Technologies. – 2014. – Vol. 25 (1). – P. 41–55.

241. An effective Blockchain- based, decentralized application for smart building system management / Q. Xu [et al.] // Time Data Analytics for Large Scale Sensor Data. – 2020. – P. 157–181. – DOI: 10.1016/B978-0-12-818014-3.00008-5.

242. Atlam, H. Intersections between IoT and distributed ledger / H. Atlam, G. Wills // Advances in Computers. – 2019. – Vol. 115. – P. 74–113. – DOI: 10.1016/bs.adcom.2018.12.001.

243. Blockchain – based IoT: A Survey / R. Thakore [et al.] // Procedia Computer Science. – 2019. – Vol. 155. – P. 704–709. – DOI: 10.1016/j.procs.2019.08.101.

244. NSA Prism program taps in to user data of Apple, Google and others. – 2013. – URL: http://www.theguardian.com/world/2013/jun/06/us-techgiants-nsa-data (date of access: 09.02.2019).

245. Hassan, M. Privacy preservation in Блокчейн based IoT systems: Integration issues, prospects, challenges, and future research directions / M. Hassan, M. Rehmani, J. Chen // Future Generation Computer Systems. – 2019. – Vol. 97. – P. 512285–529. – DOI: 10.1016/j.future.2019.02.060.

246. Empowering the edge-practical insights on a decentralized internet of things / P. Veena [et al.] // IBM Institute for Business Value. – 2015. – Vol. 17. – 21 p. – URL: https://www.ibm.com/downloads/cas/2NZLY7XJ (date of access: 07.08.2019).

247. On Blockchain and its integration with IoT. Challenges and opportunities / A. Reyna [et al.] // Future Generation Computer Systems. – 2018. – Vol. 88. – P. 173–190. – DOI: 10.1016/j.future.2018.05.046.

248. Singh, S. Block IoT Intelligence: A Blockchain-enabled Intelligent IoT Architecture with Artificial Intelligence / S. Singh, S. Rathore, J. Park // Future Generation Computer Systems. – 2020. – Vol. 110. – P. 721–743. – DOI: 10.1016/j.future.2019.09.002.

249. Diaz, M. State-of-the-art, challenges, and open issues in the integration of internet of things and cloud computing / M. Diaz, C. Martin, B. Rubio // Journal of Network and Computer Applications. – 2016. – Vol. 67. – P. 99–117.

250. Savaglio, C. Agent-based Internet of Things: State-of-the-art and research challenges / C. Savaglio, G. Fortino, M. Ganzha // Future Generation Computer Systems. – 2020. – Vol. 102 (10). – P. 1038–1053. – DOI: 10.1016/j.future.2019.09.016.

251. Multi-agent systems and Blockchain: Results from a systematic literature review / D. Calvaresi [et al.] // Intlernational Conference on Practical Applications of Agents and Multi-Agent Systems. – NY: Springer, 2018. – P. 110–126.

252. Lai, R. Blockchain – From Public to Private: Handbook of Blockchain / R. Lai, D. Lee, K. Chuen // Digital Finance, and Inclusion. – 2018. – Vol. 2. – P. 146–177. – DOI: 10.1016/B978-0-12-812282-2.00007-3.

253. A Case Study for Blockchain in Manufacturing: "FabRec": A Prototype for Peer-to-Peer Network of Manufacturing Nodes / A. Angrish [et al.] // Procedia Manufacturing. – 2018. – Vol. 26. – P. 1180–1192.

254. Swan, M. Blockchain for Business: Next- Generation Enterprise Artificial Intelligence Systems / M. Swan // Advances in Computers. – 2018. – Vol. 111. – P. 121–162. – DOI: 10.1016/bs.adcom.2018.03.013.

255. Mougayar, W. The business Blockchain: Promise, practice and application of the next internet technology / W. Mougayar. – New Jersey: Wiley, 2016. – 208 p.

256. Consensus mechanisms and information security technologies / P. Zhang [et al.] // Advances in Computers. – 2019. – Vol. 115. – P. 181–209. – DOI: 10.1016/bs.adcom.2019.05.001.

257. A new type of Blockchain for secure message exchange in VANET / R. Shrestha [et al.] // Digital Communications and Networks. – 2020. – Vol. 6 (2). – P. 177–186. – DOI: 10.1016/j.dcan.2019.04.003.

258. Larimer, D. Delegated proof of stake / D. Larimer. – 2014. – URL: www.bitshares.org (date of access: 19.10.2019).

259. Castro, M. Practical Byzantine Fault tolerance Miguel / M. Castro, B. Liskov // Proceeding Third Symposium on Operating Systems Design and Implementation. – 2002. – P. 114.

260. Theodorou, S. Blockchain Based Security and Privacy in Smart Cities / S. Theodorou, N. Sklavos // Smart Cities Cybersecurity and Privacy. – 2019. – Chapter 3. – P. 21–37. – DOI: 10.1016/B978-0-12-815032-0.00003-2.

261. King, S. PPCoin: peer-to-peer crypto-currency with proof-of-stake / S. King, S. Nadal. – 2012. – URL: https://peercoin.net/assets/paper/peercoin-paper.pdf (date of access: 14.04.2019).

262. Consortium Blockchains: Overview, applications and challenges / O. Dib [et al.] // International Journal on Advances in Telecommunications. – 2018. – Vol. 11. – P. 51–63. – URL: https://www.thinkmind.org/articles/tele_v11_n12_2018_5.pdf (date of access: 03.05.2020).

263. Clack, C. Smart contract templates: foundations, design landscape and research directions / C. Clack, V. Bakshi, L. Braine. – 2016. – 15 p. – URL: https://arxiv.org/pdf/1608.00771.pdf (date of access: 29.11.2019).

264. Guadamuz, A. All watched over by machines of loving grace: A critical look at smart contracts / A. Guadamuz // The International Journal of Technology Law and Practice. – 2019. – Vol. 35 (6). – P. 1–16. – DOI: 10.10167j.clsr.2019.105338.

265. Szabo, N. Smart contracts Building Blocks for Digital Markets / N. Szabo. – 1996. – URL: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html (date of access 23.03.2019).

266. Zheng, Z. An overview on smart contracts: Challenges, advances and platforms / Z. Zheng, S. Xie, H.-N. Dai // Future Generation Computer Systems. – 2019. – Vol. 105. – P. 1–19. – DOI: 10.1016/j.future.2019.12.019.

267. Meunier, S. Blockchain 101: What is Blockchain and How Does This Revolutionary Technology Work? / S. Meunier // Transforming Climate Finance and Green Investment with Blockchains. – Cambridge: Elsevier Inc., 2018. – P. 23–34. – DOI: 10.1016/B978-0-12-814447-3.00003-3.

268. Dissecting ponzi schemes on ethereum: identification, analysis, and impact / M. Bartoletti [et al.] // Future Generation Computer Systems. – 2020. – Vol. 102. – P. 259–277. – DOI:10.1016/j.future.2019.08.014.

269. Zhang, P. Blockchain solutions for healthcare / P. Zhang, N. Maged, K. Boulos // Precision Medicine for Investigators, Practitioners and Providers. – 2020. – P. 519–524. – DOI: 10.1016/B978-0-12-819178-1.00050-2.

270. Applying software patterns to address interoperability in blockchain-based healthcare apps / P. Zhang [et al.]. – June 5, 2017. – 17 p. – URL: arXiv:1706.03700 (date of access: 17.06.2019).

271. Cachin, C. Architecture of the Hyperledger Blockchain Fabric / C. Cachin // Workshop on Distributed Cryptocurrencies and Consensus

Ledgers. – 2016. – 4 p. – URL: https://www.zurich.ibm.com/dccl/papers/cachin_dccl.pdf (date of access: 16.04.2019).

272. Brown, R. The Corda platform: An introduction / R. Brown. – 2018. – 21 p. – URL: https://www.corda.net/content/corda-platform-whitepaper.pdf (date of access: 31.01.2019).

273. Mazieres, D. The Stellar consensus protocol: A federated model for internet-level consensus / D. Mazieres. – 2016. – 32 p. – URL: https://assets.website-files.com/5deac75ecad2173c2ccccbc7/5df2560fba2fb0526f0ed55f_stellar-consensus-protocol.pdf (date of access: 28.04.2020).

274. Lerner, D. Rootstock whitepaper / D. Lerner. – 2015. – 23 p. – URL: https://docs.rsk.co/RSK_White_Paper-Overview.pdf (date of access: 11.10.2021).

275. Pustisek, M. Approaches to Front-End IoT Application Development for the Ethereum Blickchain / M. Pustisek, A. Kos // Procedia Computer Science. – 2018. – Vol. 129. – P. 410–419. – DOI:10.1016/j.procs.2018.03.017.

276. IBM Watson Internet of Things. Blockchain and IoT: Vending Machine with eSIM Demo. – 2017. – URL: https://www.youtube.com/watch?v=T9kYuBcOnjI (date of access: 22.12.2021).

277. Davidson, S. Blockchains and the economic institutions of capitalism / S. Davidson, P. De Filippi, J. Potts // Journal of Institutional Economics. – 2018. – Vol. 13 (4). – P. 639–658.

278. Blockchain and the evolution of institutional technologies: Implications for innovation policy / D. Allen [et al.] // Research Policy. – 2020. – Vol. 49 (1). – 24 p. – DOI: 10.1016/j.respol.2019.103865.

279. Catalini, C. Some Simple Economics of the Blockchain: Rotman School of Management / C. Catalini, J. Gans // MIT Sloan Research Paper No. 519116. – 2016. – 39 p. – URL: https://ssrn.com/abstract = 2874598 (date of access: 05.01.2022).

280. Luther, W. Cryptocurrencies, network effects, and switching costs / W. Luther // Contemporary Economic Policy. – 2016. – Vol. 34 (3). – P. 553–571.

281. Langlois R., Robertson P. Firms, Markets and Economic Change: A Dynamic Theory of Business Institutions / R. Langlois, P. Robertson. – London: Routledge, 1995. – 200 p.

282. Duchenne, J. Blockchain and Smart Contracts: Complementing Climate Finance, Legislative Frameworks, and Renewable Energy Projects / J. Duchenne // Transforming Climate Finance and Green

Investment with Blockchains. – 2018. – Chapter 22. – P. 303–317. – DOI: 10.1016/B978-0-12-814447-3.00022-7.

283. Schmidt, C. Blockchain and supply chain relations: A transaction cost theory perspective / C. Schmidt, S. Wagner // Journal of Purchasing and Supply Management. – 2019. – Vol. 25 (4). – P. 1–13. – DOI: 10.1016/j.pursup.2019.100552.

284. Blockchain research, practice and policy: Applications, benefits, limitations, emerging research themes and research agenda / L. Hughes [et al.] // International Journal of Information Management. – 2019. – Vol. 49. – P. 114–129. – DOI: 10.1016/j.ijinfomgt.2019.02.005.

285. Lacity, M. Addressing key challenges to making enterprise Blockchain applications a reality / M. Lacity // MIS Quarterly Executive. – 2018. – Vol. 17 (3). – P. 201–222.

286. Michelman, P. Seeing beyond the blockchain hype / P. Michelman // MIT Sloan Management Review. – 2017. – Vol. 58 (4). – P. 17–22.

287. A Blockchain-based collocation storage architecture for data security process platform of WSN / L. Fengi [et al.] // Paper Presented at the Proceedings of the 2018: 22nd International Conference on Computer Supported Cooperative Work in Design, IEEE. – 2018. – P. 39–44.

288. Guo, Y. Blockchain application and outlook in the banking industry / Y. Guo, C. Liang // Financial Innovation. – 2016. – Vol. 24. – P. 1–12. – DOI: 10.1186/s40854-016-0034-9.

289. Blockchain for and in logistics: What to adopt and where to start / M. Dobrovnik [et al.] // Logistics. – 2018. – Vol. 2 (3). – P. 1–14. – DOI: 10.3390/logistics2030018.

290. Holub, M. Bitcoin research across disciplines / M. Holub, J. Johnson // The Information Society. – 2018. – Vol. 34 (2). – P. 114–126.

291. Wright, T. Deloitte: 39% of Companies Worldwide Now Have Blockchain in Production / T. Wright. – URL: https://cointelegraph.com/news/deloitte-39-of-companies-worldwide-now-have-Blockchain-in-production (date of access: 17.06.2020).

292. Blockchain in healthcare: challenges and solutions / M. Onik [et al.] // Big Data Analytics for Intelligent Healthcare Management. – Cambridge: Elsevier Inc., 2019. – P. 197–226. – DOI: 10.1016/B978-0-12-818146-1.00008-8.

293. McGoogan, C. The end of passport gates? Dubai to test ‘invisible’ airport checks using facial recognition / C. McGoogan // The Telegraph. – 2017. – URL: http://www.telegraph.co.uk/technology/2017/06/13/end-passport-gates-dubai-test-invisible-airport-checks-using/ (date of access: 03.10.2020).

294. E-identity. – 2017. – URL: https://e-estonia.com/solutions/e-identity/e-residency/ (date of access: 03.10.2020).

295. How to get an Illinois Birth Certificate online. – 2017. – URL: https://vital-records.us/order-an-illinois-birth-certificate/ (date of access: 04.10.2020).

296. Chandran, R. Indian states look to digitize land deals with Blockchain / R. Chandran // Reuters. – 2017. – URL: https://www.reuters.com/article/us-india-landrights-tech/indian-states-look-to-digitize-land-deals-with-blockchain-idUSKBN1AQ1T3 (date of access: 16.10.2020).

297. Browne, R. Blockchain Technology Being Considered by More Than Half of Big Corporations, According to Study / R. Browne // CNBC. – 2017. – URL: https://www.cnbc.com/2017/07/31/blockchain-technology-considered-by-57-percent-of-big-corporations-study.html (date of access: 09.05.2019).

298. Perez, Y. Santander: Blockchain Tech Can Save Banks $20 Billion a Year / Y. Perez. – 2015. – URL: https://www.coindesk.com/business/2015/06/16/santander-blockchain-tech-can-save-banks-20-billion-a-year/ (date of access: 16.06.2015).

299. Iansiti, M. The truth about Blockchain / M. Iansiti, K. Lakhani // Harvard Business Review. – 2017. – Vol. 95 (1). – P.118–127.

300. Drescher, D. Blockchain basics: A non-technical introduction in 25 steps / D. Drescher. – Frankfurt am Main: Apress, 2017. – 270 p.

301. Rabah, K. Overview of Blockchain as the engine of the 4th industrial revolution / K. Rabah // Mara Research Journal of Business & Management. – 2017. – Vol. 1 (1). – P. 125–135.

302. Securing IoTs in distributed Blockchain: Analysis, requirements and open issues / S. Moin [et al.] // Future Generation Computer Systems. – 2019. – Vol. 100. – P. 325–343. – DOI: 10.1016/j.future.2019.05.023.

303. Blockchain Challenges and Opportunities: A Survey / Z. Zheng [et al.] // International Journal of Web and Grid Services. – 2018. – Vol. 14 (4) – P. 352–375.

304. Bitcoin: Economics, technology, and governance / R. Bohme [et al.] // The Journal of Economic Perspectives. – 2015. – Vol. 29 (2). – P. 213–238.

305. Coyne, J. Can blockchains serve an accounting purpose? / J. Coyne, P. McMickle // Journal of Emerging Technologies in Accounting. – 2017. – Vol. 14 (2). – P. 101–111.

306. Lynn, T. Legitimizing #Blockchain: An empiriпcal analysis of firm level social media messaging on Twitter: 26th European Conference on Information Systems (ECIS 2018) / T. Lynn, P. Rosati, G. Fox – 2018. – 17 p.

307. Risius, M. A Blockchain research framework / M. Risius, K. Spohrer // Business & Information Systems Engineering. – 2017. – Vol. 59 (6). – P. 385–409.

308. Yeoh, P. Regulatory issues in blockchain technology / P. Yeoh // Journal of Financial Regulation and Compliance. – 2017. – Vol. 25 (2). – P. 196–208.

309. Biswas, B. Analysis of barriers to implement Blockchain in industry and service sectors / B. Biswas, R. Gupta // Computers & Industrial Engineering. – 2019. – Vol. 136. – P. 225–241. DOI: 10.1016/j.cie.2019.07.005.

310. Babich, V. Distributed ledgers and operations: what operations management researchers should know about Blockchain technology / V. Babich, G. Hilary // Manufacturing & Service Operations Management. – 2020. – Vol. 22 (2). – P. 1–18. – DOI: 10.1287/msom.2018.0752.

311. Angelis, J. Blockchain adoption: A value driver perspective / J. Angelis, E. da Silva // Business Horizons. – 2019. – Vol. 62. – P. 307–314. – DOI: 10.1016/j.bushor.2018.12.001.

312. Swan, M. Blockchain: Blueprint for a new economy / M. Swan. – Sebastopol, CA: O'Reilly Media. 2015. – 128 p. – URL: http://book.itep.ru/depository/blockchain/blockchain-by-melanie-swan.pdf (date of access: 16.10.2020).

313. Schuster, B. What is the third generation of Blockchain technology? / B. Schuster // HackerNoon. – URL: https://hackernoon.com/what-is-the-third-generation-of-blockchain-technology-36a46af5ccbc (date of access: 26. 01.2018).

314. Maersk and IBM to form joint venture applying blockchain to improve global trade and digitize supply chains / IBM. – 2018. – URL: https://newsroom.ibm.com/2018-01-16-Maersk-and-IBM-to-Form-Joint-Venture-Applying-Blockchain-to-Improve-Global-Trade-and-Digitize-Supply-Chains (date of access: 16.01.2018).

315. Wass, S. Trade finance blockchain platform soon available to clients of nine European banks / S. Wass. – 2018. – URL: https://www.gtreview.com/news.fintech/trade-finance-blockchain-platform-soon-available-to-clients-of- nine-european-banks/ (date of access: 25.10.2021).

316. Raval, S. Decentralized applications / S. Raval. – Sebastopol, CA: O'Reilly Media, 2016. – 104 p.

317. Harris, P. What blockchain technology means for artificial intelligence / P. Harris; NASDAQ. – 2017. – URL: https://www.nasdaq.com/article/analysis-what-blockchain-technology-means-for-artificial-intelligence-cm888540 (date of access: 07.12.2019).

318. Vocke, C. Application potentials of artificial intelligence for the design of innovation processes / C. Vocke, C. Constantinescu, D. Popescu // Procedia CIRP. – 2019. – Vol. 84. – P. 810–813. – DOI: 10.1016/j.procir.2019.04.230.

319. The European Commission's High-Level Expert Group on Artificial Intelligence: A Definition of AI: Main Capabilities and Scientific Disciplines. – Brussels, 2018. – 9 p. – URL: https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf (date of access: 08.03.2021).

320. Savaglio, C. Agent-based Internet of Things: State-of-the-art and research challenges / C. Savaglio, G. Fortino, M. Ganzha // Future Generation Computer Systems. – 2020. – Vol. 102 (C). – P. 1038–1053. – DOI: 10.1016/j.future.2019.09.016.

321. Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. Opinion paper / Y. Dwivedi [et al.] // International Journal of Information Management. – 2021. – Vol. 57 (7). – 97 p. – DOI: 10.1016/j.ijinfomgt.2019.08.002.

322. Jain, P. Artificial intelligence in flexible manufacturing systems / P. Jain, C. Mosier // International Journal of Computer Integrated Manufacturing. – 1992. – Vol. 5 (6). – P. 378–384.

323. Intelligent manufacturing in the context of Industry 4.0: A review / R. Zhong [et al.] // Engineering. – 2017. – No. 3 (5). – P. 616–630.

324. Combining the power of artificial intelligence with the richness of healthcare claims data: Opportunities and challenges / D. Thesmar [et al.] // PharmacoEconomics. – 2019. – Vol. 37 (4). – P. 745–752. – DOI: 10.1007/s40273-019-00777-6.

325. AI in Retail: Segment analysis, vendor positioning and market forecasts 2019–2023: Juniper Research, 2018. – URL: https://www.giiresearch.com/report/jp372628-ai-artificial-intelligence-machine-learning-retail.html (date of access: 13.09.2019).

326. Wang, L. Outlook of cloud, CPS and IoT in manufacturing. Cloud-based cyber-physical systems in manufacturing / L. Wang, X. Wang. – Cham: Springer, 2016. – P. 377–398.

327. PricewaterhouseCoopers Wirtschaftsprufungsgesellschaf GmbH: Kunstliche Intelligenz als Innovationsbeschleuniger in Unternehmen – Zuversicht und Vertrauen in Kunstliche Intelligenz. – Stuttgart, 2018. – 21 p. – URL: https://www.pwc.de/de/digitale-transformation/kuenstliche-intelligenz/kuenstliche-intelligenz-als-innovationsbeschleuniger-im-unternehmen.pdf (date of access: 25.10.2020).

328. Chandrinos, S. AIRMS: A risk management tool using machine learning / S. Chandrinos, G. Sakkas, N. Lagaros // Expert Systems with Applications. – 2018. – Vol. 105. – P. 34–48.

329. Sanford, A. Operational risk modeling and organizational learning in structured finance operations: A Bayesian network approach / A. Sanford, I. Moosa // Journal of the Operational Research Society. – 2015. – Vol. 66 (1). – P. 86–115.

330. IDC Forecasts Improved Growth for Global AI Market in 2021. – 2021. – URL: https://www.idc.com/getdoc.jsp?containerId=prUS46794720 (date of access: 25.08.2020).

331. Notes from the AI Frontier – Modeling the Impact of AI on the World Economy / J. Bughin [et al.]; McKinsey Global Institute, Brussels, San Francisco, Shanghai, Stockholm. – 2018. – 64 p. – URL: https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Artificial%20Intelligence/Notes%20from%20the%20frontier%20Modeling%20the%20impact%20of%20AI%20on%20the%20world%20economy/MGI-Notes-from-the-AI-frontier-Modeling-the-impact-of-AI-on-the-world-economy-September-2018.ashx (date of access: 05.06.2020).

332. Hawksworth, J. AI and robots could create as many jobs as they displace / J. Hawksworth. – 2018. – URL: https://www.weforum.org/agenda/2018/09/ai-and-robots-could-create-as-many-jobs-as-they-displace/ (date of access: 18.09.2018).

333. Andriole, S. Artificial intelligence, China and the U.S. – How the U.S. is losing the technology war / S. Andriole // Forbes. – 2018. – URL: https://www.forbes.com/sites/steveandriole/2018/11/09/artificial-intelligence-china-and-the-us-how-the-us-is-losing-the-technology-war/#2dcafacd6195 (date of access: 03.02.2020).

334. Многогранный интеллект: использование ИИ в промышленности, образовании и ритейле // Tass.ru. – 2021. – Октябрь. – Режим доступа: https://tass.ru/obschestvo/12584775 (дата обращения: 25.10.2021).

335. Jobs lost, jobs gained: Workforce transitions in a time of automation / J. Manyika [et al.]; McKinsey Global Institute. – 2017. –

28 p. – URL: https://www.mckinsey.com/~/media/mckinsey/industries/public%20and%20social%20sector/our%20insights/what%20the%20future%20of%20work%20will%20mean%20for%20jobs%20skills%20and%20wages/mgi-jobs-lost-jobs-gained-executive-summary-december-6-2017.pdf (date of access: 26.04.2018).

336. DIN&DKE German standardization roadmap Industrie 4.0. V 3. – 2018. – URL: https://www.din.de/blob/65354/57218767bd6da1927b181b9f2a0d5b39/roadmap-i4-0-e-data.pdf (date of access: 03.02.2020).

337. Jonsson, A. Systematic lead time analysis / A. Jonsson, V. Svensson; Chalmers University of Technology. – 2016. – 97 p. – URL: https://publications.lib.chalmers.se/records/fulltext/238746/238746.pdf (date of access: 01.09.2020).

338. Heinen, N. Artificial Intelligence and Human Labour: Implications for Companies and Economic Policy / N. Heinen, A. Heuer, P. Schautschick // Wirtschaftsdienst. – 2017. – P. 714–720. – DOI: 10.1007/s10273-017- 2203-5.

339. Big data: The next frontier for innovation, competition, and productivity. – Lexington, KY: McKinsey & Company, 2011. – 156 p. – URL: https://www.mckinsey.com/~/media/mckinsey/business functions/mckinsey digital/our insights/big data the next frontier for innovation/mgi_big_data_full_report.pdf (date of access: 23.06.2021).

340. Kaur, P. Big Data and Machine Learning Based Secure Healthcare Framework / P. Kaur, M. Sharma, M. Mittal // Procedia Computer Science. – 2018. Vol. 132. – P. 1049–1059. – DOI:10.1016/j.procs.2018.05.020.

341. Mneney, J. Big data capabilities and readiness of south african retail organisations / J. Mneney, J.-P. Van Belle // Cloud system and big data engineering (conluence): 6th international conference IEEE. – Uttar Pradesh, India, 2016. – P. 279–286. – DOI: 10.1109/CONFLUENCE.2016.7508129.

342. Addressing big data issues in scientific data infrastructure / Y. Demchenko [et al.] // Collaboration technologies and systems (CTS): IEEE International conference. – San Diego, 2013. – P. 48–55. – DOI: 10.1109/CTS.2013.6567203.

343. Saggi, M. A survey towards an integration of big data analytics to big insights for value-creation / M. Saggi, S. Jain // Information Processing & Management. – 2018. – Vol. 54 (5). – P. 758–790. – DOI: 10.1016/j.ipm.2018.01.010.

344. Gandomi, A. Beyond the hype: Big data concepts, methods, and analytics / A. Gandomi, M. Haider // International Journal of Information Management. – 2015. – Vol. 35 (2). – P. 137–144.

345. Aguilar, S. Learning analytics: At the nexus of big data, digital innovation, and social justice in education / S. Aguilar // TechTrends. – 2018. – Vol. 62 (1). – P. 37–45. – DOI: 10.1007/s11528-017-0226-9.

346. Dorasamy, N. Social impact and social media analysis relating to Data science and big data computing / N. Dorasamy, N. Pomazalova // Data Science and Big Data Computing: ed. Z. Mahmood. – Cham: Springer, 2016. – P. 293–313. – DOI: 10.1007/978-3-319-31861-5.

347. Sagiroglu, S. Big data: A review / S. Sagiroglu, D. Sinanc // Collaboration technologies and systems (CTS): IEEE International conference. – San Doego, 2013. – P. 42–47. – DOI:10.1109/ CTS.2013.6567202.

348. Raguseo, E. Big data technologies: An empirical investigation on their adoption, benefits and risks for companies / E. Raguseo // International Journal of Information Management. – 2018. – Vol. 38 (1). – P. 187–195. – DOI: 10.1016/j.ijinfomgt.2017.07.008.

349. Baesens, B. Analytics in a big data world: The essential guide to data science and its applications / B. Baesens. – New Jersey: John Wiley & Sons, 2014. – 256 p.

350. Philip, J. An application of the dynamic knowledge creation model in big data / J. Philip // Technology in Society. – 2018. – Vol. 54. – P. 120–127. – DOI: 10.1016/j.techsoc.2018.04.001.

351. Machine Learning based Digital Twin Framework for Production Optimization in Petrochemical Industry / Q. Min [et al.] // International Journal of Information Management. – 2019. – Vol. 49. – P. 502–519. – DOI: 10.1016/j.ijinfomgt.2019.05.020.

352. Big data reduction framework for value creation in sustainable enterprises / M. Rehman [et al.] // International Journal of Information Management. – 2016. – Vol. 36. – P. 917–928.

353. Tellaeche, A. Machine learning algorithms for quality control in plastic molding industry / A. Tellaeche, R. Arana // Emerging Technologies & Factory Automation (ETFA): 18th Conference / IEEE. – Cagliari, 2013. – P. 1–4.

354. Big data: From beginning to future / I. Yaqoob [et al.] // International Journal of Information Management. – 2016. – Vol. 36. – P. 1231–1247.

355. Big Data in the construction industry: A review of present status, opportunities, and future trends / M. Bilal [et al.] // Advanced engineering informatics. – 2016. – Vol. 30. – P. 500–521.

356. From data to value: A nine-factor framework for data-based value creation in information-intensive services / C. Lim [et al.] // International Journal of Information Management. – 2018. – Vol. 39. – P. 121–135.

357. Mamonov, S. The strategic value of data resources in emergent industries / S. Mamonov, T. Triantoro // International Journal of Information Management. – 2018. – Vol. 39. – P. 146–155.

358. A Big Data system supporting Bosch Braga Industry 4.0 strategy / M. Santos [et al.] // International Journal of Information Management. – 2017. – Vol. 37. – P. 750–760.

359. Automatic detection of relationships between banking operations using machine learning / I. Gonzalez-Carrasco [et al.] // Information Sciences. – 2019. – Vol. 485. – P. 319–346. – DOI: 10.1016/j.ins. 2019.02.030.

360. Lee, I. Big data: Dimensions, evolution, impacts, and challenges / I. Lee // Business Horizons. – 2017. – Vol. 60 (3). – P. 293–303. – DOI: 10.1016/j.bushor.2017.01.004.

361. Davenport, T. Big data at work: Dispelling the myths, uncovering the opportunities / T. Davenport. – Boston: Harvard Business Review Press, 2014. – 228 p.

362. Accenture. Big data analytics in supply chain: Hype or here to stay? – 2016. – URL: https://www.accenture.com (date of access: 13.12.2021).

363. House, J. Big data analytics = Key to successful 2015 supply chain strategy / J. House // ModusLink. – 2015. – URL: https:// www.moduslink.com/big-data-analytics-key-successful-2015-supply-chain-strategy/ (date of access: 09.11.2018).

364. The Financial Brand. Big data: Profitability potential, and problems in banking. – 2014. – URL: http://thefinancialbrand.com/ 38801/big-data-profi tability-strategy-analytics-banking/ (date of access: 15.08.2019).

365. Doku, R. Big Data in Cybersecurity for Smart City Applications / R. Doku, D. Rawat // Smart Cities Cybersecurity and Privacy. – 2019. – Chapter 8. – P. 103–112. – DOI: 10.1016/B978-0-12-815032-0.00008-1.

366. Kaplan, A. Users of the world, unite! The challenges and opportunities of social media / A. Kaplan, M. Haenlein // Business Horizons. – 2010. – Vol. 53 (1). – P. 59–68.

367. Van Rijmenam, M. Tesco and big data analytics, a recipe for success? / M. van Rijmenam // Datafloq. – 2016. – URL: https://

datafloq.com/ read/tesco-big-data-analytics-recipe-success/665 (date of access: 15.08.2019).

368. Osman, A. A novel big data analytics framework for smart cities / A. Osman // Future Generation Computer Systems. – 2019. – Vol. 91. – P. 620–633. – DOI: 10.1016/j.future. 2018.06.046.

369. Chase, R. Peers Inc: How People and Platforms Are Inventing the Collaborative Economy and Reinventing Capitalism / R. Chase. – NY: PublicAffairs, 2015. – 306 p. – URL: https://opexsociety.org/ bookstore/peers-inc-people-platforms-inventing-collaborative-economy-reinventing-capitalism/ (date of access: 22.04.2021).

370. Gawer, A. Bridging differing perspectives on technological platforms: Toward an integrative framework / A. Gawer // Research Policy. – 2014. – Vol. 43. – P. 1239–1249. – DOI:10.1016/j.respol. 2014.03.006.

371. Rochet, J.-C. Two-sided markets: a progress report. / J. C. Rochet, J. Tirole // RAND Journal of Economics. – Vol. 37 (3) – 2006. – P. 645–667.

372. Evans, D. Some empirical aspects of multi-sided platform industries / D. Evans // Review of Network Economics. – 2003. – Vol. 2 (3). – P. 1–19. – DOI: 10.2202/1446-9022.1026.

373. Rysman, M. The economics of two-sided / M. Rysman // Journal of Economic Perspectives. – 2009. – Vol. 23. – P. 125–143.

374. Armstrong, M. Competition intwo-sided markets / M. Armstrong // RAND Journal of Economics. – 2006. – Vol. 37 (3). – P. 668–691.

375. Макарова, Ю. Подождите на платформе: как защитить права фрилансеров и самозанятых / Ю. Макарова // РБК. Тренды. – Режим доступа: https://trends.rbc.ru/trends/social/cmrm/60b494449a7947202aa63cc1?utm_source=ss_tg_rbc&utm_medium=tg&utm_campaign=ss_tg_rbc (дата обращения: 30.06.2021).

376. Hagiu A., Wright J. Multi-sided platform: Working Paper No. 12024 / A. Hagiu, J. Wright. – Harvard: Harvard Business School, 2011. – 5 p.

377. Parker, G. Two-sided network effects: a theory of information product / G. Parker, M. van Alstyne // Management Science. – 2005. – Vol. 51. – P. 1494 –1504.

378. Eisenmann, T. Opening platforms: how, when, and why? / T. Eisenmann, G. Parker, M. van Alstyne // Platforms, Markets and Innovation / ed. A. Gawer. – Cheltenham, UK: Mass, 2009. – P. 131–162.

379. Evans, P. The Rise of the Platform Enterprise: A Global Survey / P. Evans, A. Gawer. – New York: Center for Global Enterprise, 2016. – 30 p. – URL: http://www.thecge.net/wp-content/uploads/2016/01/PDF-WEB-Platform-Survey_01_12.pdf (date of access: 22.04.2021).

380. Asset Management as a Digital Platform Industry: A Global Financial Network Perspective / D. Haberly [et al.] // Geoforum. – 2019. – Vol. 106. – P. 167–181. – DOI: 10.1016/j.geoforum.2019.08.009.

381. Edelman, B. Efficiencies and regulatory shortcuts: how should we regulate companies like AirBNB and Uber? / B. Edelman, D. Geradin // Stanford Technology Law Review. – 2015. – Vol. 19 (2). – P. 293–328.

382. Hazlett, T. Walled garden rivalry: the creation of mobile network ecosystems: George Mason University Law and Economics Research Paper Series No. 11-50 / T. Hazlett, D. Teece, L. Waverman. – 2011. – 31 p. – URL: https://www.law.gmu.edu/assets/files/publications/working_papers/1150WalledGardenRivalry.pdf (date of access: 22.02.2019).

383. A New School in Chicago // The Economist. – 2018. – URL: https://www.economist.com/special-report/2018/06/28/how-regulators-can-prevent-excessive-concentration-online (date of access: 28.06.2018).

384. More Knock-On than Network // The Economist. – 2018. – URL: https://www.economist.com/special-report/2018/06/28/the-story-of-the-internet-is-all-about-layers (date of access: 28.06.2018).

385. Eisenmann, T. Strategies for two sided markets/ T. Eisenmann, G. Parker, M. van Alstyne // Harvard Business Review. – 2006. – Vol. 84. – P. 92–101.

386. Cramer-Flood, E. In global historic first, ecommerce in China will account for more than 50% of retail sales / E. Cramer-Flood. – 2021. – URL: https://www.emarketer.com/content/global-historic-first-ecommerce-china-will-account-more-than-50-of-retail-sales (date of access: 10.02.2021).

387. Ecosystem 2.0: Climbing to the next level / V. Chung [et al.] // McKinsey Quaeterly. – 2020. – 9 p. – URL: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Ecosystem%202%20point%200%20Climbing%20to%20the%20next%20level/Ecosystem-2-point-0-Climbing-to-the-next-level.pdf (date of access: 06.12.2021).

388. Lessig, L. Code, Version 2.0 / L. Lessig. – New York: Basic Books, 2006. – 410 p.

389. Райзберг, Б. А. Современный экономический словарь / Б. А. Райзберг, Л. Ш. Лозовский, Е. Б. Стародубцева. – М.: ИНФРА-М, 1999. – 479 с.

390. The new economy: beyond the hype: Final report on the OECD growth project meeting of the OECD council at ministerial level. – 2021. – 28 p. – URL: https://www.oecd.org/economy/growth/2380634.pdf (date of access: 14.12.2021).

391. Aydin, E. A Study of Superiority of E-Trade Compared to Traditional Methods of Commerce in Overcoming Crises: Case Study of kitapix.com / E. Aydin, S. Kavaklioglu // Procedia Social and Behavioral Sciences. – 2011. – № 24. – P. 123–137.

392. Новикова, И. В. Геоэкономика как «Новая мировая сетевая экономика» / И. В. Новикова. – Saarbrucken: Pelmarium Academic Publishing, 2016. – 70 с.

393. Дрогобыцкий, И. А. Системный анализ в экономике: учеб. пособие / И. А. Дрогобыцкий. – М.: Финансы и статистика: ИНФРА-М, 2009. – 512 с.

394. A conceptual approach to analysing manufacturing companies' profiles concerning Industry 4.0 in emerging economies / D. Horvat [et al.] // Procedia Manufacturing. – 2018. – Vol. 17. – P. 419–426.

395. Industry 4.0: The Future of Productivity and Growth in Manufacturing Industries / M. Rusmann [et al.] // Boston Consulting Group. – 09.04.2015. – URL: https://www.bcg.com/publications/2015/engineered_products_project_business_industry_4_future_productivity_growth_manufacturing_industries (date of access: 13.06.2019).

396. Monostori, L. Cyber-physical production systems / L. Monostori // Procedia CIRP. – 2014. – Vol. 17. – P. 9–13.

397. Lee, J. A cyber-physical systems architecture for industry 4.0-based manufacturing systems / J. Lee, B. Bagheri, H. Kao // Manufacturing. – 2015. – Vol. 3. – P. 18–23.

398. Andelfinger, V. Industrie 4.0: Wie cyber-physische Systeme die Arbeitswelt verandern (How cyber-physical systems change working environment) / V. Andelfinger, T. Hanisch. – Wiesbaden, Germany: Springer Gabler, 2017. – 271 p.

399. Reference architectures for smart manufacturing: A critical review / M. Moghaddam [et al.] // Journal of Manufacturing Systems. – 2018. – Vol. 49. – P. 215–225. – DOI: 10.1016/j.jmsy.2018.10.006.

400. Kagermann, H. Securing the future of german manufacturing industry: Recommendations for implementing the strategic initiative

INDUSTRIE 4.0.: Final report of the Industrie 4.0. Working Group / H. Kagermann, W. Wahlster, J. Helbig. – 2013. – 78 p. – URL: https://docplayer.net/254711-Securing-the-future-of-german-manufacturing-industry-recommendations-for-implementing-the-strategic-initiative-industrie-4-0.html (date of access: 28.11.2019).

401. German Federal Ministry for Economic Affairs and Energy, Standardization Administration of the P.R.C. 2018: Alignment Report for Reference Architectural Model for Industrie 4.0 // Intelligent Manufacturing System Architecture. – 2018. – 35 p. – URL: https://www.dke.de/resource/blob/1711304/2e4d62811e90ee7aad10eeb6fdeb33d2/alignment-report-for-reference-architectural-model-for-industrie-4-0-data.pdf (date of access: 21.10.2021).

402. Cyber-physical systems alter automation architectures / M. Riedl [et al.] // Annual Reviews in Control. – 2014. – Vol. 38. – P. 123–133. – URL: https://coek.info/pdf-cyber-physical-systems-alter-automation-architectures-.html (date of access: 09.04.2019).

403. How virtualization, Decentrazliation and network building change the manufacturing landscape: An industry 4.0 perspective / M. Keller [et al.] // International Journal of Computer and Communication Engineering. – 2014. – Vol. 8 (1). – P. 37–44.

404. Goldman, D. China is first out of the gate to Industry 4.0 / D. Goldman. – 2021. – URL: https://asiatimes.com/2021/06/china-is-first-out-of-the-gate-to-industry-4-0/ (date of access: 26.06.2021).

405. Smart manufacturing operations planning and control program. Gaithersburg: National Institute of Standards and Technology (NIST). – 2017. – URL: https://www.nist.gov/programs-projects/smart-manufacturing-operations-planning-and-control-program (date of access: 18.08.2021).

406. Driving unconventional growth through the industrial internet of things. Accenture Technology / P. Daugherty [et al.]. – 2015. – 20 p. – URL: https://www.dematec.com.au/assets/accenture-driving-unconventional-growth-through-iiot.pdf (date of access: 21.07.2021).

407. Schumacher, A. A maturity model for assessing Industry 4.0 readiness and maturity of manufacturing enterprises / A. Schumacher, S. Erol, W. Sihn // Procedia CIRP. – 2016. – Vol. 52. – P. 161–166.

408. Veža, I. Evaluation of Industrial Maturity Level: A Case Study of Croatia / I. Veža, M. Marko, N. Gjeldum // The 26th International Conference on Flexible Automation & Intelligent Manufacturing / Dong-Won, Kim. – Seoul: Science and Technology Center, 2016. – P. 467–473.

409. Mladineo, M. Case Study of Croatian manufacturing industry: Industry 4.0 Providers or Users? / M. Mladineo, D. Horvat, I. Veza // 6th International Conference Mechanical Technologies and Structural Materials-MTSM. – Split, 2016. – URL: https://www.researchgate.net/publication/349692708_Case_Study_of_Croatian_manufacturing_industry_Industry_40_Providers_or_Users (date of access: 29.11.2019).

410. Matt, C. Digital transformation strategies / C. Matt, T. Hess, A. Benlian // Business & Information Systems Engineering. – 2015. – Vol. 57. – P. 339–343.

411. Providing industry 4.0 technologies: The case of a production technology cluster / G. Dalmarco [et al.] // The Journal of High Technology Management Research. – 2019. – Vol. 30 (2). – 9 p. – DOI: 10.1016/j.hitech.2019.100355.

412. Grote, G. A. Beyond human-centred automation – Concepts for human – machine interaction in multi-layered networks / G. Grote, J. Weyer, N. A. Stanton // Ergonomics. – 2014. – Vol. 57 (3). – P. 289–294. – DOI: 10.1080/00140139.2014.890748.

413. Fitzgerald, J. Using autonomous robots to drive supply chain innovation: Deloitte / J. Fitzgerald. – 2018. – URL: https://www2.deloitte.com/us/en/pages/manufacturing/articles/autonomous-robots-supply-chain-innovation.html (date of access: 23.02.2020).

414. National Geographic. Meet the Cobots: Humans and Robots Together on the Factory Floor. – 2016. – URL: https:// news.nationalgeographic.com/2016/05/financial-times-meet-the-cobots-humans-robots-factories/ (date of access: 20.12.2018).

415. IFR presents World Robotics 2021 reports / IFR. – 2021. – URL: https://ifr.org/ifr-press-releases/news/robot-sales-rise-again; https://ifr.org/downloads/press2018/2021_10_28_WR_PK_Presentation_long_version.pdf (date of access: 28.10.2021).

416. Toffler, A. The Third Wave / A. Toffler. – Toronto: Bantam Books, 1981. – 537 p.

417. Kotler, P. «Prosumer: A new type of customer» / P. Kotler // Futurist. – 1986. – P. 24–28.

418. Jiang, R. Predicting the future of additive manufacturing: A Delphi study on economic and societal implications of 3D printing for 2030 / R. Jiang, R. Kleer, F. Piller // Technological Forecasting & Social Change. – 2017. – Vol. 117. – P. 84–97. – DOI: 10.1016/j.techfore.2017.01.006.

419. Rayna, T. From rapid prototyping to home fabrication: how 3D printing is changing business model innovation / T. Rayna, L. Striukova // Technological Forecasting and Social Change. – 2016. – Vol. 102. – P. 214–224.

420. Mellor, S. Additive manufacturing: A framework for implementation / S. Mellor, L. Hao, D. Zhang // International Journal of Production Econopmics. – 2014. – Vol. 149. – P. 194–201. – DOI: 10.1016/j.ijpe.2013.07.008.

421. Connected baby bottle: a design case study towards a framework for data-enabled design / S. J. A. Bogers [et al.] // 11th ACM Conference on Designing Interactive Systems (DIS 2016) / Eindhoven MedTech Innovation Center. – 4 Jun. 2016. – P. 301–311. – URL: https://research.tue.nl/en/publications/connected-baby-bottle-a-design-case-study-towards-a-framework-for/fingerprints/ (date of access: 16.08.2019).

422. Berman, B. 3-D printing: The new industrial revolution / B. Berman // Business Horizons. – 2012. – Vol. 55. – P. 155–162. – DOI: 10.1016/j.bushor.2011.11.003.

423. Rapid manufacturing in the spare parts supply chain: Alternative approaches to capacity deployment / J. Holmstrom [et al.] // Journal of Manufacturing Technology Management. – 2010. – Vol. 21. – P. 687–697. – DOI: 10.1108/17410381011063996.

424. Digital Shadow Platform as an Innovative Business Model / J. Stecken [et al.] // Procedia CIRP. – 2019. – Vol. 83. – P. 204–209. – DOI: 10.1016/j.procir.2019.02.130.

425. Banerjee, A. Blockchain Technology: Supply Chain Insights from ERP / A. Banerjee // Advances in Computers. – 2018. – Vol. 111. – P. 69–98. – DOI: 10.1016/bs.adcom.2018.03.007.

426. Bauernhansl, T. WGP-Standpunkt Industrie 4.0. WGP: Wissenschaftliche Gesellschaft fur Produktionstechnik / T. Bauernhansl. – Darmstadt, 2016. – 29 p. – URL: https://www.ipa.fraunhofer.de/content/dam/ipa/de/documents/Presse/Presseinformationen/2016/Juni/WGP_Standpunkt_Industrie_40.pdf (date of access: 16.08.2019).

427. Glaessgen, E. The digital twin paradigm for future NASA and US Air Force vehicles / E. Glaessgen, D. Stargel // 53rd AIAA/ASME/ASCE/AHS/ASC Structural Dynamics and Materials Conference. – Honolulu, Hawaii, 2012. – 14 p. –DOI: 10.2514/6.2012-1818.

428. Cloud manufacturing: a new service-oriented networked manufacturing model / B. Li [et al.] // Computer Integrated Manufacturing Systems. – 2010. – Vol. 16. – P. 1–7.

429. Bohu, L. Introduction to cloud manufacturing / L. Bohu, Z. Lin, C. Xudong // ZTE Communications Technology. – 2010. – Vol. 4. – P. 5–8.

430. Grieves, M. Digital Twin: Manufacturing Excellence Through Virtual Factory Replication: Florida Institute of Technology / M. Grieves. – 2014. – 8 p. – URL:https://www.3ds.com/fileadmin/PRODUCTS-SERVICES/DELMIA/PDF/Whitepaper/DELMIA-APRISO-Digital-Twin-Whitepaper.pdf (date of access: 13.10.2020).

431. Service-oriented manufacturing: a new product pattern and manufacturing paradigm / J. Gao [et al.] // Journal of Intelligent Manufacturing. – 2011. – Vol. 22 (3). – P. 435–446. – DOI: 10.1007/s10845-009-0301-y.

432. Brocal, F. Advanced Manufacturing Processes and Technologies / F. Brocal, M. Sebastian, C. Gonzalez // Management of Emerging Public Health Issues and Risks. – 2019. – P. 31–64. – DOI: 10.1016/B978-0-12-813290-6.00002-0.

433. Cloud computing – The business perspective / S. Marston [et al.] // Decision Support Systems. – 2011. – Vol. 51 (1). – P. 176–189. – DOI: 10.1016/J.DSS.2010.12.006.

434. Industrial blockchain based framework for product lifecycle management in industry 4.0 / X. Liu [et al.] // Robotics and Computer Integrated Manufacturing. – 2020. – Vol. 63 (C). – P. 1–16. – DOI: 10.1016/j.rcim.2019.101897.

435. Cloud-based design and manufacturing: a new paradigm in digital manufacturing and design innovation / D. Wu [et al.] // Computer-Aided Design. – 2015. – Vol. 59. – P. 1–14. – DOI: 10.1016/j.cad.2014.07.006.

436. Bahga, A. Blockchain platform for industrial internet of things / A. Bahga, V. Madisetti // Journal of Software Engineering and Applications. – 2016. – Vol. 9 (10). – P. 533–546. – DOI: 10.4236/jsea.2016.910036.

437. Carvalho, H. Lean, agile, resilient and green: Divergencies and synergies / H. Carvalho, S. Duarte, V. Machado // International Journal of Lean Six Sigma. –2011. – Vol. 2. – P. 151–179. – DOI: 10.1108/20401461111135037.

438. Ozdogru, U. Impact of exponential technologies on global supply chain management / U. Ozdogru // Technology in Supply Chain Management and Logistics. – 2020. – Chapter 3. – P. 37–55. – DOI: 10.1016/B978-0-12-815956-9.00003-X.

439. Lee, I. The Internet of Things (IoT): Applications, investments, and challenges for enterprises / I. Lee, K. Lee // Business Horizons. – 2015. – Vol. 58. – P. 431–440. – DOI: 10.1016/j.bushor.2015.03.008.

440. Agile Supply Chain Management over the Internet of Things / L. Ping [et al.] // Management and Service Science (MASS). – Wuhan, China, 2011. – 4 p. – DOI: 10.1109/ICMSS.2011.5998314.

441. Sustainability in multi-tier supply chains: understanding the double agency role of their first-tier supplier / M. Wilhelm [et al.] // Journal of Operations Management. – 2016. – Vol. 41. – P. 42–60.

442. Blockchain technology and enterprise operational capabilities: An empirical test / X. Pan [et al.] // International Journal of Information Management. – 2020. – Vol. 52 (C). – 9 p. – DOI: 10.1016/j.ijinfomgt. 2019.05.002.

443. Information system capabilities and firm performance: Opening the black box through decision-making performance and business process performance / A. Aydiner [et al.] // International Journal of Information Management. – 2019. – Vol. 47 (8). – P. 168–182.

444. Min, H. Blockchain technology for enhancing supply chain resilience / H. Min // Business Horizons. – 2019. – Vol. 62 (1). – P. 35–45. – DOI: 10.1016/j.bushor.2018.08.012.

445. Maruti Techlab. What is Blockchain and understand its benefits. – 2017. – URL: https://www.marutitech.com/keyblockchain-benefits/ (date of access: 25.06.2021).

446. Takahashi, R. How can creative industries benefit from blockchain? / R. Takahashi; McKinsey & Company. – 2017. – URL: https:// www.mckinsey.com/industries/media-and-entertainment/our-insights/ how-can-creative-industries-benefit-from-blockchain (date of access: 19.11.2019).

447. Ballou, R. The evolution and future of logistics and supply chain management / R. Ballou // European Business Review. – 2007. – Vol. 19. – P. 332–348. – DOI: 10.1108/09555340710760152.

448. Banerjee, A. Blockchain with IoT: Applications and use cases for a new paradigm of supply chain driving efficiency and cost / A. Banerjee // Advances in Computers. – 2019. – Vol. 115. – P. 260–292. – DOI: 10.1016/bs.adcom.2019.07.007.

449. Beyond Bitcoin: What Blockchain and distributed ledger technologies mean for firms / A. Hughes [et al.] // Business Horizons. – 2019. – Vol. 62. – P. 273–281. DOI: 10.1016/j.bushor.2019.01.002 0007-6813.

450. Boucher, P. How Blockchain technology could change our lives / P. Boucher. – Brussels, Belgium: European Parliamentary Research Service, 2017. – 28 p. – URL: https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf (date of access: 06.09.2019).

451. SAP. – 2018. – URL: https://www.sap.com/products/supply-chain-iot/scm.html (date of access: 02.09.2019).

452. CISCO. – 2018. – URL: https://www.cisco.com/c/dam/en/us/solutions/collateral/digital-transformation/supply-chain-digital-age.pdf?dtid5osscdc000283 (date of access: 21.03.2021).

453. Кочетов, А. Логистические кейсы / А. Кочетов // РБК. – 2021. – Режим доступа: https://plus.rbc.ru/news/60740e0e7a8aa90f59023b3b (дата обращения: 11.01.2022).

454. Искусственный интеллект, роботы и электромобили: что ждет логистику в ближайшем будущем? – 2021. – Режим доступа: https://vc.ru/u/667561-ab-inbev-efes/318380-iskusstvennyy-intellekt-roboty-i-elektromobili-chto-zhdet-logistiku-v-blizhayshem-budushchem (дата обращения: 12.11.2021).

455. Moise, I. Maersk and IBM Partner on Blockchain for global trade / I. Moise, D. Chopping // The Wall Street Journal. – 2018. – URL: https://www.wsj.com/articles/maersk-and-ibm-partner-on-blockchain-for-global-trade-1516111543?mod=searchresults&page=2&pos=18 (date of access: 24.02.2020).

456. Maersk and IBM Introduce TradeLens Blockchain Shipping Solution PRNewswire. – 2016. – URL: https://newsroom.ibm.com/2018-08-09-Maersk-and-IBM-Introduce-TradeLens-Blockchain-Shipping-Solution (date of access: 27.08.2020).

457. Global Trade and Digitise Supply Chains. – 2018. – URL: https://www.maersk.com/press/press-release-archive/maersk-and-ibm-to-form-joint-venture (date of access: 3.02.2020).

458. Higgins, S. Automaker Renault Trials Blockchain in Bid to Secure Car Repair Data / S. Higgins. – 2017. – URL: https://www.coindesk.com/automaker-renault-trials-blockchain-bid-secure-car-repair-data/ (date of access: 12.02.2018).

459. Gimenez-Escalante, P. Innovative Food Technologies for Redistributed Manufacturing Technologies (SMART) / P. Gimenez-Escalante, S. Rahimifard; Centre for Sustainable Manufacturing & Recycling. – Loughborough: Loughborough University, 2016. – 50 p. – URL: https://repository.lboro.ac.uk/ndownloader/files/17211356/1 (date of access: 27.08.2020).

460. Srai, J. Characteristics of redistributed manufacturing systems: a comparative study of emerging industry supply networks / J. Srai, T. Harrington, M. Tiwari // International Journal of Production Research. – 2016. – Vol. 54 (23). – P. 6936–6955.

461. Developing manufacturing ontologies for knowledge reuse in distributed manufacturing environment / L. Lin [et al.] // International Journal of Production Research. – 2011. – Vol. 49 (2). – P. 343–359.

462. A CBFSA approach to resolve the distributed manufacturing process planning problem in a supply chain environment / N. Mishra [et al.] // International Journal of Production Research. – 2012. – Vol. 50 (2). – P. 535–550.

463. Yadav, G. A fuzzy AHP approach to prioritize the barriers of integrated Lean Six Sigma / G. Yadav, T. N. Desai // International Journal of Quality & Reliability Management. – 2017. – Vol. 34 (8). – P. 1167–1185.

464. Adapting an agile manufacturing concept to the reference architecture model industry 4.0: A survey and case study / M. Yli-Ojanpera [et al.] // Journal of Industrial Information Integration. – 2019. – Vol. 15. – P. 147–160. – DOI:10.1016/j.jii.2018.12.002.

465. Xu, L. Industry 4.0: State of the art and future trends / L. Xu, E. Xu, L. Li // International Journal of Production Research. – 2018. – Vol. 56 (8). – P. 2941–2962.

466. Modeling opportunistic IoT services in open IoT ecosystems / G. Fortino [et al.] // XVIII Workshop From Objects to Agents. – June 2017. – P. 90–95. – URL: http://ceur-ws.org/Vol-1867/w16.pdf (date of access: 31.03.2021).

467. Karadayi-Usta, S. An interpretive structural analysis for industry 4.0 adoption challenges / S. Karadayi-Usta // IEEE Transactions on Engineering Management. – 2020. – Vol. 67 (3). – P. 973–978. – DOI: 10.1109/tem.2018.2890443.

468. Hermann, M. Design principles for Industrie 4.0 scenarios / M. Hermann, T. Pentek, B. Otto // Proceedings of the annual Hawaii international conference on system sciences. – 2016. – P. 3928–3937. – DOI: 10.1109/HICSS.2016.488.

469. Factories of the future: Multi-annual roadmap for the contractual PPP under Horizon 2020 / EFFRA. – Brussels: Publications Office of the European Union, 2013. – 136 p. – URL: https://www.effra.eu/sites/default/files/factories_of_the_future_2020_roadmap.pdf (date of access: 11.01.2022).

470. Huxtable, J. On servitization of the manufacturing industry in the UK / J. Huxtable, D. Schaefer // Procedia CIRP. – 2016. – Vol. 52. – P. 46–51.

471. What is new in the new industrial policy? A manufacturing systems perspective / E. O'Sullivan [et al.] // Oxford Review of Economic Policy. – 2013. – Vol. 29 (2). – P. 432–462. – DOI: 10.1093/oxrep/grt027.

472. France. Industry of the future: Rallying the new face of industry in France. – 2015. – 76 p. – URL: https://www.economie.gouv.fr/files/nouvelle_france_industrielle_english.pdf (date of access: 27.08.2020).

473. Netherlands. Smart industry: Dutch industry fit for the future. – 2017. – 33 p. – URL: https://wp.kennisbanksocialeinnovatie.nl/wp-content/uploads/2020/08/Smart-Industry.pdf (date of access: 24.05.2021).

474. Italy: "Industria 4.0". – 2017. – 8 p. – URL: https://ati.ec.europa.eu/sites/default/files/2020-06/DTM_Industria4.0_IT%20v2wm.pdf (date of access: 06.08.2021).

475. Cotec. Industria 4.0. – 2017. – URL: https://cotecportugal.pt/en/projects/industry-4-0/ (date of access: 04.01.2019).

476. Smart manufacturing: past research, present findings and fu ture directions / H. Kang [et al.] // International Journal of Precision Engineering and Manufacturing – Green Technology. – 2016. – Vol. 3 (1). – P. 111–128.

477. Sung, T. Industry 4.0: a Korea perspective / T. Sung // Technological Forecasting and Social Change. – 2018. – Vol. 132. – P. 40–45.

478. Babones, S. India to Be world's Fastest Growing Economy: keeping it Going will Be the Difficult trick / S. Babones // A report by Forbes. – 2018. – URL: https://www.forbes.com/sites/salvatorebabones/2018/01/10/india-may-be-the-worlds-fastest-growing-economy-but-regional-disparity-is-a-serious-challenge/?sh=3b6c0a5d53ac (date of access: 04.02.2020).

479. Molnar, M. The US Advanced Manufacturing Initative / M. Molnar. – 2017. – 44 p. – URL: https://www.nist.gov/system/files/documents/2017/04/28/Molnar_091211.pdf (date of access 31.12.2019).

480. Deutsches Institut fúr Normung (DIN). Industry 4.0: New ISO Strategic 2015 / Advisory Group. – January 12, 2018. – URL: https://www.din.de/en/innovation-and-research/industry-4-0/industry-4-0-new-iso-strategic- advisory-group-66486 (date of access: 15.10.2020).

481. Industry 4.0 a Study for the European Parliament / J. Smit [et al.]. – 2016. – 94 p. – URL: http://www.europarl.europa.eu/RegData/

etudes/STUD/2016/570007/IPOL_STU(2016)570007_EN.pdf (date of access: 05.05.2020).

482. Betti, F. The Fourth Industrial Revolution and manufacturing's great reset / F. Betti, E. de Boer, Y. Giraud / McKinsey&Company. – Sepember 2020. – 5 p. – URL: https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Operations/Our%20Insights/The%20Fourth%20Industrial%20Revolution%20and%20manufacturings%20great%20reset/The-Fourth-Industrial-Revolution-and-manufacturings-great-reset-vF.pdf (date of access: 23.02.2021).

483. Zillner, S. Towards intelligent manufacturing, semantic modelling for the steel industry / S. Zillner, A. Ebel, M. Schneider // IFAC-Papers Online. – 2016. – Vol. 49 (20). – P. 220–225. – DOI: 10.1016/j.ifacol.2016.10.124.

484. Ganzarain, J. Three stage maturity model in SME's towards industry 4.0 / J. Ganzarain, N. Errasti // Journal of Industrial Engineering and Management. – 2016. – Vol. 9 (5). – P. 1119–1128. – DOI:10.3926/jiem.2073.

485. Preparing for the next normal via digital manufacturing's scaling potential / E. de Boer [et al.]; McKinsey Operations Practice. – April 2020. – P. 10. – URL: https://www.mckinsey.com/business-functions/operations/our-insights/preparing-for-the-next-normal-via-digital-manufacturings-scaling-potential#download/%2F~%2Fmedia%2Fmckinsey%2Fbusiness%20functions%2Foperations%2Four%20insights%2Fpreparing%20for%20the%20next%20normal%20via%20digital%20manufacturings%20scaling%20potential%2Fpreparing-for-the-next-normal-via-digital-manufacturings-scaling-potential.pdf%3FshouldIndex%3Dfalse (date of access: 07.01.2021).

486. Leveraging industry 4.0 – A business model pattern framework / J. Weking [et al.] // International Journal of Production Economics. – 2020. – Vol. 225. – 17 p. – DOI: 10.1016/j.ijpe.2019.107588.

487. Urquhart, L. Avoiding the Internet of insecure industrial things / L. Urquhart, D. McAuley // Computer Law & Security Review. – 2018. – Vol. 34 (3). – P. 450–466. – DOI: 10.1016/j.clsr.2017.12.004.

488. Customer centricity as key for the digital breakthrough / M. Becker [et al.]; McKinsey Company and VDMA. – September 2020. – 68 p. – URL: https://www.mckinsey.com/~/media/McKinsey/Industries/Advanced%20Electronics/Our%20Insights/Digitization%20How%20machinery%20companies%20can%20meet%20customers%20expectations/Digitization-How-machinery-companies-can-meet-customers-expectations.pdf (date of access: 24.03.2021).

489. Klerkx, L. Dealing with the game-changing technologies of Agriculture 4.0: How do we manage diversity and responsibility in food system transition pathways? / L. Klerkx, D. Rose // Global Food Security. – 2020. – Vol. 24. – 7 p. – DOI: 10.1016/j.gfs.2019.100347.

490. Rose, D. Agriculture 4.0: broadening responsible innovation in an Era of smart farming / D. Rose, J. Chilvers // Frontiers in Sustainable Food Systems. – 2018. – Vol. 2. – P. 1–7. – DOI: 10.3389/fsufs.2018.00087.

491. Revolution 4.0: Industry vs. Agriculture in a future development for SMEs / I. Zambon [et al.] // Processes. – 2019. – Vol. 7 (1). – 16 p. – DOI: 10.3390/pr7010036.

492. Hermans, F. The potential contribution of transition theory to the analysis of bioclusters andtheir rolein thetransition toabioeconomy / F. Hermans // Biofuels, Bioproducts and Biorefining. – 2018. – Vol. 12. – P. 265–276.

493. Strategic points in aquaponics / R. Junge [et al.] // Water. – 2017. – Vol. 9 (3). – 9 p. – DOI: 10.3390/w9030182.

494. Pigford, A.-A. Beyond agricultural innovation systems? Exploring an agricultural innovation ecosystems approach for niche design and development in sustainability transitions / A.-A. Pigford, G. Hickey, L. Klerkx // Agricultural Systems. – 2018. – Vol. 164. – P. 116–121.

495. Pinstrup-Andersen, P. Is it time to take vertical indoor farming seriously? / P. Pinstrup-Andersen // Global Food Security. – 2018. – Vol. 17. – P. 233–235.

496. De Wilde, S. The Future of Technology in Agriculture: STT Netherlands Study Centre for Technology Trends / S. De Wilde. – The Netherlands: The Hague, 2016. – 118 p. – URL: http://maisagro.pt/wp-content/uploads/2017/06/grp04_the_future_of_technology_in_agriculture.pdf (date of access: 06.11.2019).

497. Burton, R. The potential impact of synthetic animal protein on livestock production: the new “war against agriculture”? / R. Burton // Journal of Rural Studies. – 2019. – Vol. 68. – P. 33–45.

498. De Clercq, M. Agriculture 4.0: the Future of Farming Technology: World Government Summit / M. De Clercq, A. Vats, A. Biel. – 2018. – 30 p. – URL: https://www.worldgovernmentsummit.org/api/publications/document?id=95df8ac4-e97c-6578-b2f8-ff0000a7ddb6 (date of access: 09.10.2019).

499. The future of food 2040 / NFU. – 2019. – URL: https://www.nfuonline.com/nfu-online/news/the-future-of-food-2040 (date of access: 19.02.2020).

500. An intelligent Edge-IoT platform for monitoring livestock and crops in a dairy farming scenario / R. Alonso [et al.] // Ad Hoc Networks. – 2019. – Vol. 98 (3). – 53 p. – DOI: 10.1016/j.adhoc.2019.102047.

501. Big data in smart farming-a review / S. Wolfert [et al.] // Agricultural Systems. – 2017. – Vol. 153. – P. 69–80.

502. Wolfert, S. A future internet collaboration platform for safe and healthy food from farm to fork / S. Wolfert, D. Goense, C. Sorensen // Annual SRII Global Conference / IEEE. – 2014 – P. 266–273.

503. Toward quantified small-scale farms in Africa / K. Fleming [et al.] // IEEE Internet Computing. – 2016. – Vol. 20. – P. 63–67.

504. Kethareswaran, V. An Indian perspective on the adverse impact of internet of things (IoT) / V. Kethareswaran, C. Ram // Advances in Distributed Computing and Artificial Intelligence Journal. – 2017. – Vol. 6 (4). – P. 35–40.

505. Patil, K. A model for smart agriculture using IoT / K. Patil, N. Kale // International Conference on Global Trencs in Signal Processing, Information Computing and Communication. – 2016. – P. 543–545.

506. Internet of things platform for smart farming: Experiences and lessons learnt / P. Jayaraman [et al.] // Sensors. – 2016. – Vol. 16 (11). – 17 p. – DOI: 10.3390/s16111884.

507. Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges / I. Mistry [et al.] // Mechanical Systems and Signal Processing. – 2020. – Vol. 135. – 21 p. – DOI: 10.1016/j.ymssp.2019.106382.

508. Munir, M. An intelligent and secure smart watering system using fuzzy logic and Blockchai / M. Munir, I. Bajwa, S. Cheema // Computers and Electrical Engineering. – 2019. – Vol. 77. – P. 109–119. – DOI: 10.1016/j.compeleceng.2019.05.006.

509. Internet of Things (IoT): a vision, architectural elements, and future directions / G. Jayavardhana [et al.] // Future Generation Computer Systems. – 2013. – Vol. 29. – P. 1645–1660. – DOI: 10.1016/j.future.2013.01.010.

510. Agricultural Robotics: The Future of Robotic Agriculture. UK-RAS White papers, EPSRC UK Robotics and Autonomous Systems Network. – London, 2018. – 36 p. – URL: https://www.n8agrifood.ac.uk/

media/dx-tile/Future-of-robotics-agriculture-1.pdf (date of access: 30.04.2020).

511. Brown, M. Digitalization of Energy / M. Brown, S. Woodhouse, F. Sioshansi // Consumer, Prosumer, Prosumager. – 2019. – Chapter 1. – P. 3–25. – DOI: 10.1016/B978-0-12-816835-6.00001-2.

512. Review of Technologies and Platforms for Smart Cities / F. de 'a Prieta [et al.] // Advances in Intelligent Systems and Computing. – NY: Springer International Publishing, 2019. – P. 193–200.

513. A framework for blockchain based secure smart green house farming / A. S. Patil [et al.] // Advances in Computer Science and Ubiquitous Computing. – NY: Springer, 2017. – P. 1162–1167.

514. Dileep, G. survey on smart grid technologies and applications / G. Dileep // Renewable Energy. – 2020. – Vol. 146. – P. 2589–2625. – DOI: 10.1016/j.renene.2019.08.092.

515. Diestelmeier, L. Changing power: Shifting the role of electricity consumers with blockchain technology – Policy implications for EU electricity law / L. Diestelmeier // Energy Policy. – 2019. – Vol. 128. – P. 189–196. – DOI: 10.1016/j.enpol.2018.12.065.

516. Khalilpour, K. Design and Operational Management of Energy Hubs: A DS4S (Screening, Selection, Sizing, and Scheduling) Framework / K. Khalilpour // Polygeneration with Polystorage. – 2019. – Chapter 15. – P. 493–512. – DOI: 10.1016/B978-0-12-813306-4.00015-X.

517. Khalilpour, K. Community energy networks with storage: modeling frameworks for distributed generation / K. Khalilpour, A. Vassallo. – Singapore: Springer; 2016. – 191 p.

518. Khalilpour, K. A generic framework for DGS nanogrids / K. Khalilpour, A. Vassallo // Community energy networks with storage: modeling frameworks for distributed generation. – Singapore: Springer; 2016. – P. 41–59.

519. Aggregated battery control for peer-to-peer Energy sharing in a community Microgrid with PV battery systems / C. Long [et al.] // Energy Procedia. – 2018. – Vol. 145. – P. 522–527.

520. Blockchain – based microgrid gives power to consumers in New York. – 2017. – URL: https://www.newscientist.com/article/2079334-blockchain-based-microgrid-gives-power-to-consumers-in-new-york/ (date of access: 03.05.2019).

521. Bitcoin-inspired peer-to-peer solar trading trial kicks off in Perth. – 2017. – URL: http://reneweconomy.com.au/bitcoin-inspired-peer-to-peer-solar-trading-trial-kicks-off-in-perth-29362/ (date of access: 06.09.2021).

522. Introducing Piclo. – 2017. – URL: https://www.openutility.com/product/ (date of access: 11.03.2022).

523. An online marketplace for energy; a world first in The Netherlands / Vandebron. – 2017. – URL: http://vandebron.pr.co/72191-an-online-marketplace-for-energy-a-world-first-in-the-netherlands (date of access: 16.06.2021).

524. Zhang, R. New challenges to power system planning and operation of smart grid development in China / R. Zhang, Y. Du, L. Yuhong // International Conference on Power System Technology. – Zhejiang, China, 2010. – P. 1–8. –DOI: 10.1109/POWERCON.2010.5666114.

525. Sharma, P. Blockchain based hybrid network architecture for the Smart city / P. Sharma, J. Park // Future Generation Computer Systems. – 2018. – Vol. 86. – P. 650–655. – DOI: 10.1016/j.future.2018.04.060.

526. Jenks, M. A sustainable future through the compact city? Urban intensification in the United Kingdom / M. Jenks, E. Burton, K. Williams // Environment by Design. – 1996. – Vol. 1 (1). – P. 5–20.

527. Lam, P. Potential pitfalls in the development of smart cities and mitigation measures: An exploratory study / P. Lam, R. Ma // Cities. – 2018. – Vol. 91. – P. 146–156. – DOI: 10.1016/j.cities.2018.11.014.

528. Merry, H. Population increase and the smart city / H. Merry. – 2017. – URL: https://www.ibm.com/blogs/internet-of-things/increased-population-smart-city/ (date of access: 25.02.2020).

529. Приоритетные направления внедрения технологий умного города в российских городах: экспертно-аналитический доклад / Центр стратегических разработок «Пространственное развитие», Центр стратегических разработок «Северо-Запад». – М., июнь 2018. – 178 с. – Режим доступа: https://www.csr.ru/upload/iblock/bdc/bdc711b002e9651fb2763d98c7f7daa6.pdf (дата обращения: 01.04.2021).

530. Zanella, A. Internet of things for smart cities / A. Zanella // IEEE Internet Things Journal. – 2014. – Vol. 1 (1). – P. 22–32.

531. Lemstra, W. Leadership with 5G in Europe: Two contrasting images of the future, with policy and regulatory implications / W. Lemstra // Telecommunications Policy. – 2018. – Vol. 42 (8). – P. 587–611. – DOI: 10.1016/j.telpol.2018.02.003.

532. Longzhi, Y. Privacy and Security Aspects of E-Government in Smart Cities / Y. Longzhi, E. Noe, E. Neil // Smart Cities Cybersecurity and Privacy. – 2019. – Chapter 7. – P. 89–102. – DOI: 10.1016/B978-0-12-815032-0.00007-X.

533. Mohanty, S. P. Everything you wanted to know about smart cities: the Internet of Things is the backbone / S. P. Mohanty, U. Choppali, E. Kougianos // IEEE Consumer Electronics Magazine. – 2016. – Vol. 5 (3). – P. 60–70.

534. Marsal-Llacuna, M.-L. Lessons in urban monitoring taken from sustainable and livable cities to better address the smart cities initiative / M.-L. Marsal-Llacuna, J. Colomer-Llinas, J. Melendez-Frigola // Technological Forecasting and Social Change. – 2015. – Vol. 90. – P. 611–622.

535. Rush, K. Digital Glasgow Roadmap / K. Rush. – 2014. – 28 p. – URL: https://www.glasgow.gov.uk/CHttpHandler.ashx?id=18230&p=0 (date of access: 05.02.2012).

536. Amsterdam Smart City. – URL: https://amsterdamsmartcity.com/ (date of access: 01.02.2020).

537. Paulin, A. Digitalized Governance – An Embezzled Opportunity? / A. Paulin // Smart City Governance. – 2019. – Chapter 2. – P. 39–60. – DOI: 10.1016/B978-0-12-816224-8.00002-9.

538. Anthopoulos, L. Defining smart city architecture for sustainability / L. Anthopoulos // Proceedings of the 14th IFIP Electronic Government (EGOV) and 7th Electronic Participation (EPart) Conference 2015. Presented at the 14th IFIP Electronic Government and 7th Electronic Participation Conference 2015. – Thessaloniki, Greece: IOS Press, 2015. – P. 140–147. – DOI: 10.3233/978-1-61499-570-8-140.

539. Cooley, D. Next decade to bring fourfold increase in number of smart cities / D. Cooley. – 2016. – URL: https://smartcitiescouncil.com/article/next-decade-bring-fourfold-increase-number-smart-cities (date of access: 10.11.2020).

540. Boussoufa-Lahlah, S. Geographic routing protocols for Vehicular Ad hoc NETworks (VANETs): a survey / S. Boussoufa-Lahlah, F. Semchedine, L. Bouallouche-Medjkoune // Vehicular Communications. – 2018. – Vol. 11. – P. 20–31.

541. Kim, S. Blockchain for a Trust Network Among Intelligent Vehicles / S. Kim // Advances in Computers. – 2018. – 26 p. – DOI: 10.1016/bs.adcom.2018.03.010.

542. Papathanassiou, A. Cellular V2X as the essential enabler of-superior global connected transportation services / A. Papathanassiou, A. Khoryaev // IEEE 5G Tech Focus. – 2017. – Vol. 1 (2). – URL: https://futurenetworks.ieee.org/tech-focus/june-2017/cellular-v2x (date of access: 09.07.2021).

543. Kenney, J. Dedicated short-range communications (DSRC) standards in the United States / J. Kenney // Proceedings of the IEEE. – 2011. – Vol. 99 (7). – P. 1162–1182.

544. Connected world: An evolution in connectivity beyond the 5G revolution: Discussion paper / F. Grijpink [et al.]; McKinsey Global Institute February. – 2020. – 100 p. – URL: https://www.mckinsey.com/~/media/McKinsey/Industries/Technology%20Media%20and%20Telecommunications/Telecommunications/Our%20Insights/Connected%20world%20An%20evolution%20in%20connectivity%20beyond%20the%205G%20revolution/MGI_Connected-World_Discussion-paper_February-2020.pdf (date of access: 09.07.2021).

545. Mobility's future: An investment reality check / D. Holland-Letz [et al.]; McKinsey Center for Future Mobility. – April 2021. – 9 p. – URL: https://www.mckinsey.com/~/media/McKinsey/Industries/Automotive%20and%20Assembly/Our%20Insights/Mobilitys%20future%20An%20investment%20reality%20check/Mobilitys-future-An-investment-reality-check.pdf?shouldIndex=false (date of access: 19.11.2021).

546. Dawei, L. Big Data Technology: Aplication and Cases. Handbook of Blockchain / L. Dawei, H. Anzi, L. Gen // Digital Finance, and Inclusion. – 2018. – Vol. 2. – P. 66–81. – DOI: 10.1016/B978-0-12-812282-2.00004-8 (date of access: 10.12.2020).

547. King, R. Finance and growth: Schumpeter might be right / R. King, R. Levine // The Quarterly Journalof Economics. – 1993. – Vol.108 (3). – P. 717–737.

548. Levine, R. Stock market development and long-run growth / R. Levine, S. Zervos // World Bank Economic Review. – 1996. – Vol. 10 (2). – P. 323–339.

549. Goldsmith, R. Financial Structure and Development (Study in Comparative Economics) / R. Goldsmith. – New Haven, CT: Yale University Press, 1969. – 561 p. – URL: https://www.nber.org/system/files/chapters/c4417/c4417.pdf (date of access: 12.08.2020).

550. Bernier, M. Financial innovation, economic growth, and the consequences of macro prudential policies / M. Bernier, M. Plouffe // Research in Economics. – 2019. – Vol. 73. – P. 162–173. – DOI: 10.1016/j.rie.2019.04.003.

551. Financial innovation: the bright and the dark sides / T. Beck [et al.] // Journal of Banking & Finance. – 2016. – Vol. 72 (1). – P. 28–51.

552. Casanova, L. Banks, Credit Constraints, and the Financial Technology's Evolving Role / L. Casanova, P. Cornelius, S. Dutta //

Financing Entrepreneurship and Innovation in Emerging Markets. – 2018. – Chapter 7. – P. 161–184. – DOI: 10.1016/B978-0-12-804025-6.00007-1.

553. McKinnon, R. Money and Capital in Economic Development / R. McKinnon. – Washington, D. C.: Brookings Institution Press, 1973. – 184 p.

554. Shaw, E. Financial Deepening in Economic Development / E. Shaw. – New York: Oxford University Press, 1973. – 260 p.

555. Levine, R. Financial development and economic growth: views and agenda / R. Levine // Journal of Economic Literature. – 1997. – Vol. 35. – P. 688–726.

556. Global Financial Stability Report. Grappling with Crisis Legacies: IMF Report. – 2011. – 178 p. – URL: https://www.imf.org/en/Publications/GFSR/Issues/2016/12/31/~/media/Websites/IMF/imported-flagship-issues/external/pubs/ft/GFSR/2011/02/pdf/_textpdf.ashx (date of access: 24.06.2019).

557. Securitization: Lessons Learned and the Road Ahead: IMF Working Paper WP/13/255 / M. Segoviano [et al.]. – 2013. – 74 p. – URL: https://www.imf.org/external/pubs/ft/wp/2013/wp13255.pdf (date of access: 10.01.2019).

558. Junger, M. Banking goes digital: The adoption of FinTech services by German households: Finance Research Letters / M. Junger, M. Mietzner. – 2019. – 8 p. – DOI: 10.1016/ j.frl.2019.08.008.

559. Scardovi, C. Digital Transformation in Financial Services / C. Scardovi. – London: Springer International Publishing AG, 2017. – 236 p. – DOI: 10.1007/978-3-319-66945-8.

560. Vives, X. Competition and stability in modern banking: A post-crisis perspective / X. Vives // International Journal of Industrial Organization. – 2019. – Vol. 64. – P. 55–69. – DOI: 10.1016/j.ijindorg.2018.08.011.

561. Shim, Y. Analyzing China's Fintech Industry from the Perspective of Actor-Network Theory / Y. Shim, D.-H. Shin // Telecommunications Policy. – 2016. – Vol. 40. – P. 168–181. – DOI: 10.1016/j.telpol.2015.11.005.

562. Krishnan, K. Building Big Data Aplications / K. Krishnan // Banking industry aplications and usage. – 2020. – P. 127–144. – DOI: 10.1016/B978-0-12-815746-6.00007-7.

563. Arner, D. RegTech: Building a Better Financial System / D. Arner, J. Barberis, R. Buckley // Handbook of Blockchain, Digital

Finance, and Inclusion. – 2018. – Vol. 1. – P. 359–373. – DOI: 10.1016/B978-0-12-810441-5.00016-6.

564. Patwardhan, A. Peer-To-Peer Lending / A. Patwardhan // Handbook of Blockchain, Digital Finance, and Inclusion. – 2018. – Vol. 1. – P. 390–418. – DOI: 10.1016/B978-0-12-810441-5.00018-X.

565. MSME FINANCE GAP / IFC. – 2017. – 80 p. – URL: http://www.ifc.org/wps/wcm/connect/4d6e6400416896c09494b79e78015671/Closing+the+Credit+Gap+Report-FinalLatest.pdf?MOD=AJPERES (date of access: 02.11.2020).

566. Makina, D. An overview of financial services access and usage in AFRICA / D. Makina. – 2019. – 12 p. – DOI: 10.1016/B978-0-12-814164-9.00001-3.

567. World Bank. The global findex database: Measuring financial inclusion and the FinTech revolution. – Washington DC: World Bank Publ., 2017. – 131 p. – URL: http://documents1.worldbank.org/curated/en/332881525873182837/pdf/126033-PUB-PUBLIC-pubdate-4-19-2018.pdf (date of access: 15.10.2020).

568. Koh, F. Digital Financial Inclusion in South East Asia / F. Koh, K. F. Phoon, C. D. Ha // Handbook of Blockchain, Digital Finance, and Inclusion. – 2018. – Vol. 2. – P. 387–403. – DOI: 10.1016/B978-0-12-812282-2.00015-2.

569. Kabakova, O. Analysis of factors affecting financial inclusion: Ecosystem view / O. Kabakova, E. Plaksenkov // Journal of Business Research. – 2018. – Vol. 89 (C). – P. 198–205. – DOI: 10.1016/j.jbusres.2018.01.066.

570. Mushtaq, R. Microfinance, financial inclusion and ICT: Implications for poverty and inequality / R. Mushtaq, C. Bruneau // Technology in Society. – 2019. – Vol. 59 (C). – 18 p. – DOI: 10.1016/j.techsoc.2019.101154.

571. Beck, T. Finance, inequality and the poor / T. Beck, A. Demirguc-Kunt, R. Levine // Journal of Economic Growth. – 2007. – Vol. 12 (1). – P. 27–49.

572. Loayza, N. Financial development, financial fragility, and growth / N. Loayza, R. Ranciere // Journal of Money, Credit, and Banking. – 2006. – Vol. 38 (4). – P. 1051–1076.

573. Mehrotra, A. Financial inclusion-issues for central banks / A. Mehrotra, J. Yetman. – 2015. – 14 p. – URL: https://www.bis.org/publ/qtrpdf/r_qt1503h.pdf (date of access: 13.09.2020).

574. Identifying constraints to financial inclusion and their impact on GDP and inequality: A structural framework for policy: IMF Working Paper. WP15/22 / M. Dabla-Norris [et al.]; International Monetary Fund. – 2015. – 49 p. – URтиL: https://www.imf.org/-/media/Websites/IMF/imported-full-text-pdf/external/pubs/ft/wp/ 2015/_wp1522.ashx (date of access: 14.09.2020).

575. Buera, F. The macroeconomics of microfinance: NBER Working Paper Series. W17905 / F. Buera, J. Kaboski, Y. Shin; National Bureau of Economic Research. – 2012. – 42 p. – URL: https://www.nber.org/system/files/working_papers/w17905/w17905.pdf (date of access: 30.12.2020).

576. Aghion, P. A theory of trickle-down growth and development / P. Aghion, P. Bolton // The Review of Economic Studies. – 1997. – Vol. 64 (2). – P. 151–172. – URL: https://academic.oup.com/ restud/article-pdf/64/2/151/4491029/64-2-151.pdf (date of access: 20.12.2020).

577. Digital financial inclusion and the implications for customers, regulators, supervisors and standard-setting bodies: GPFI. Issues paper. – 2014. – 24 p. – URL: https://www.gpfi.org/sites/gpfi/files/documents/Issues%20Paper%20for%20GPFI%20BIS%20Conference%20on%20Digital%20Financial%20Inclusion.pdf (date of access: 20.08.2020).

578. Carney, M. The promise of FinTech – something new under the sun? / M. Carney. – 2017. – 14 p. – URL: https://www.bis.org/review/r170126b.pdf (date of access: 02.11.2020).

579. Barberis, J. The rise of FinTech: Getting Hong Kong to lead the digital financial transition in APAC: Fintech Report / J. Barberis. – Fintech HK Publ., 2014. – 24 p.

580. Hill, J. Introduction. FinTech and the Remaking of Financial Institutions / J. Hill. – 2018. – P. 1–19. – DOI: 10.1016/b978-0-12-813497-9.00001-9.

581. Retail CBDCs. The next payments frontier: OMFIF and IBM report. – NY: IBM Corporation Publ., 2019. – 35 p.

582. Drasch, B. Integrating the «Troublemakers»: A taxonomy for cooperation between banks and fintechs / B. Drasch, A. Schweizer, N. Urbach // Journal of Economics and Business. – 2018. – Vol. 100. – P. 26–42. – DOI: 10.1016/j.jeconbus.2018.04.002.

583. The future of payments / Digital Monetary Institute. – 2020. – 68 p. – URL: https://www.omfif.org/wp-content/uploads/2020/12/The-Future-of-Payments.pdf (date of access: 11.11.2020).

584. Bradford, S. Crowdfunding and the federal securities laws / S. Bradford // Columbia Business Law Review. – 2012. – No. 1. – P. 1–150. – URL: https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2019191_code68588.pdf?abstractid=1916184&mirid=1 (date of access: 21.05.2020).

585. Галдикас, М. Будущее электронных платежных систем: 5 прогнозов о том, что будет формировать рынок в 2021 году / М. Галдикас. – 2020. – Режим доступа: https://belretail.by/article/buduschee-elektronnyih-platejnyih-sistem-prognozov-o-tom-chto-budet-formirovat-ryinok-v-godu (дата обращения: 26.07.2021).

586. Chen, K. Information asymmetry in initial coin offerings (ICOs): Investigating the effects of multiple channel signals / K. Chen // Electronic Commerce Research and Applications. – 2019. – Vol. 36. – 11 p. – DOI: 10.1016/j.elerap.2019.100858.

587. Vismara, S. Signaling to overcome inefficiencies in crowdfunding markets / S. Vismara / eds. D. Cumming, L. Hornuf // Handbook of Crowdfunding. – Palgrave, London, 2018. – P. 29–56.

588. Casanova, L. Noninstitutional Forms of Entrepreneurial Finance: Angel Investments, Accelerators, and Equity Crowdfunding / L. Casanova, P. Klaus, C. Dutta // Financing Entrepreneurship and Innovation in Emerging Markets. – 2018. – P. 239–262. – DOI: 10.1016/B978-0-12-804025-6.00010-1.

589. Huang, T. Revolution of securities law in the Internet Age: A review on equity crowd-funding / T. Huang, Y. Zhao // Computer Law & Security Review. – 2017. – Vol. 33 (6). – P. 802–810. – DOI: 10.1016/j.clsr.2017.05.016.

590. Crowdfunding's Potential for the Developing World // Information for Development Program (infoDev): The World Bank report. – 2013. – 103 p. – URL: http://www.infodev.org/infodev-files/infodev_crowdfunding_study_0.pdf (date of access: 26.07.2021).

591. Piskin, M. Islamic Online P2P Lending Platform / M. Piskin, M. Kus // Procedia Computer Science. – 2019. – Vol. 158. – P. 415–419.

592. Xu, D. China's campaign-style Internet finance governance: Causes, effects, and lessons learned for new information-based aproaches to governance / D. Xu, S. Tang, D. Guttman // Computer Law & Security Review. – 2019. – Vol. 35. – P. 3–14. – DOI: 10.1016/j.clsr.2018.11.002.

593. Salami, I. Alternative Financing Approaches and Regulation in Africa / I. Salami // Extending Financial Inclusion in Africa. – 2019. – P. 279–296. – DOI: 10.1016/B978-0-12-814164-9.00013-X.

594. Boamah, E. Techno-market fix? Decoding wealth through mobile money in the global South / E. Boamah, N. Murshid // Geoforum. – 2019. – Vol. 106. – P. 253–262.

595. Gonzalez, D. Managing Online Risk / D. Gonzalez // Apps, Mobile, and Social Media Security. – London: Butterworth-Heinemann, 2015. – P. 185–211. – DOI: 10.1016/B978-0-12-420055-5.12001-8.

596. Mobile Payments 2013 – Changing Checkout / Innopay. – 110 p. – URL: http://www.innopay.com/system/iles/private/Mobile%20payments%202013_Innopay_v1.0.pdf (date of access: 06.02.2020).

597. Miao, M. Mobile payments in Japan, South Korea and China: Cross-border convergence or divergence of business models? / M. Miao, K. Jayakar // Telecommunications Policy. – 2016. – Vol. 40 (2–3). – P. 182–196. – DOI: 10.1016/j.telpol.2015.11.011.

598. Bourreau, M. Cooperation for Innovation in Payment Systems: The Case of Mobile Payments: Telecom ParisTech Working Paper No. ESS-10-02 / M. Bourreau, M. Verdier. – 2010. – 25 p. – DOI:10.2139/ssrn.1575036.

599. Mishra, V. Mobile banking in a developing economy: A customer-centric model for policy formulation / V. Mishra, S. Bisht // Telecommunications Policy. – 2013. – Vol. 37 (6). – P. 503–514.

600. Schulte, P. Mobile Technology: The New Banking Model Connecting Lending to the Social Network / P. Schulte // Handbook of Blockchain, Digital Finance, and Inclusion. – 2018. – Vol. 2. – P. 332–329. – DOI: 10.1016/B978-0-12-812282-2.00013-9.

601. Iman, N. Is mobile payment still relevant in the fintech era? / N. Iman // Electronic Commerce Research and Applications. – 2018. – Vol. 30. – P. 72–82. – DOI: 10.1016/j.elerap.2018.05.009.

602. Evans D., Pirchio A. An empirical examination of why mobile money schemes ignite in some developing countries but flounder in most: Coase-Sandor Working Paper Series in Law and Economics, School of Law / D. Evans, A. Pirchio. – Chicago, IL University of Chicago, 2015. – No. 723. – 53 p.

603. The Mobile Financial Services Report 2011: World Economic Forum. – Cologny, Switzerland, 2011. – 223 p.

604. Mobile money, trade credit and economic development: theory and evidence: CentER Discussion Paper / T. Beck [et al.]. – Tilburg University Publications, 2015. – 49 p.

605. Duncombe, R. Mobile Phones and Financial Services in Developing Countries: A Review of Concepts, Methods, Issues, Evidence

and Future Research Directions Development Informatics: Working Paper Series / R. Duncombe, R. Boateng. – 2009. – Vol. 37. – 36 p. – URL: https://www.researchgate.net/profile/Richard-Boateng-6/publication/233439759_Mobile_Phones_and_Financial_Services_in_Developing_Countries_A_review_of_concepts_methods_issues_evidence_and_future_research_directions/links/02e7e52a8ece76d720000000/Mobile-Phones-and-Financial-Services-in-Developing-Countries-A-review-of-concepts-methods-issues-evidence-and-future-research-directions.pdf (date of access: 19.03.2020).

606. Karnouskos, S. Mobile Payment: A Journey Through Existing Procedures and Standardization Initiatives / S. Karnouskos, F. Fokus // IEEE Communications Surveys & Tutorials. – 2004. – Fourth Quarter. – P. 44–66. – URL: https://www.researchgate.net/profile/Stamatis-Karnouskos/publication/224085138_Mobile_payment_A_journey_through_existing_procedures_and_standardization_initiatives/links/0046353626a53ee797000000/Mobile-payment-A-journey-through-existing-procedures-and-standardization-initiatives.pdf (date of access: 01.03.2019).

607. Mobile Money against Financial Crimes Global Policy Challenges and Solutions: World Bank / P.-L. Chatain [et al.]. – 2011. – 235 p. – URL: https://www.researchgate.net/profile/Louis-Koker/publication/306227333_Protecting_mobile_money_against_financial_crime_global_policy_challenges_and_solutions/links/5893df08aca27231daf624f4/Protecting-mobile-money-against-financial-crime-global-policy-challenges-and-solutions.pdf (date of access: 09.03.2020).

608. Mbiti, I. The home economics of E-money: velocity, cash management, and discount rates of M-Pesa users / I. Mbiti, D. Weil // American Economic Review. – 2013. – Vol. 103 (3). – P. 369–374.

609. Mobile Money: State of the Industry Report / GSMA. – 2014. – 77 p. – URL: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2015/03/SOTIR_2014.pdf (date of access: 12.12.2019).

610. Mobile payment applications: Offer state of the Artelor in the Italian market / A. Ghezzi [et al.] // Info. – 2010. – Vol. 12 (5). – P. 3–22.

611. Nickerson, D. Diffusion of mobile payment systems among microentrepreneurs in Kenya and Tanzania / D. Nickerson; Providence College. – 2013. – 125 p. – URL: https://digitalcommons.providence.edu/cgi/viewcontent.cgi?article=1023&context=student_scholarship (date of access: 13.11.2019).

612. Okazaki, S. What do we know about mobile internet adopters? A cluster analysis / S. Okazaki // Information Management. – 2006. – Vol. 43 (2). – P. 127–146.

613. Волкова, О. Бигтехи на финансовом рынке: риски и вызовы для регуляторов / О. Волкова. – 2021. – Режим доступа: https://econs.online/articles/regulirovanie/bigtekhi-na-finansovom-rynke/ (дата обращения: 23.03.2022).

614. Bank of Ghana. Impact of Mobile Money on the Payment System in Ghana: An Econometric Analysis. – Accra, Ghana: Payment Systems Department, Bank of Ghana, 2017. – 38 p.

615. InsurTech and FinTech: Banking and Insurance Enablement / T. Yan [et al.] // Handbook of Blockchain, Digital Finance, and Inclusion. – 2018. – Vol. 1. – P. 249–281. – DOI: 10.1016/B978-0-12-810441-5.00011-7.

616. Manso, M. The Application of Telematics and Smart Devices in Emergencies / M. Manso, B. Guerra // Integration, Interconnection, and Interoperability of IoT Systems. – 2018. – P. 169–197. – DOI: 10.1007/978-3-319-61300-0_9.

617. Insurance and Technology Evolution and Revolution in a Digital World // Morgan Stanley and BGG Report. – September 2014. – 130 p. – URL: https://image-src.bcg.com/Images/evolution_revolution_how_insurers_stay_relevant_digital_world_tcm9-165956.pdf (date of access: 14.09.2020).

618. Central bank digital currencies / OMFIF, IBM Corporation. – London, Costa Mesa, 2018. – 36 p.

619. CBDC. Central bank digital currencies: foundational principles and core features: Bank for International Settlements. – 2020. – 21 p. – URL: https://www.bis.org/publ/othp33.pdf (date of access: 07.01.2022).

620. Rohr, J. Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets: Cardozo Legal Studies Research Paper No. 527 / J. Rohr, A. Wright // University of Tennessee Legal Studies Research Paper. – 2017. – No. 338. – 115 p.

621. Barrdear, J. The macroeconomics of central bank issued digital currencies/ J. Barrdear, M. Kumhof // Bank of England Staff Working Paper. – July 2016. – No. 605. – 92 p.

622. Цифровой рубль: доклад для общественных консультаций / Банк России. – М., 2020. – 48 с. – Режим доступа: https://www.cbr.ru/StaticHtml/File/112957/ Consultation_Paper_201013.pdf (дата обращения: 21.10.2020).

623. Barrdear, J. Macroeconomics of central bank issued digital currencies / J. Barrdear, M. Kumhof // FinTech and Digital Currencies Conference: BIS. – Basel, 2019. – 29 p. – URL: https://www.bis.org/events/confresearchnetwork1909/kumhof_pres.pdf (date of access: 07.09.2021).

624. Barrdear, J. Macroeconomics of central bank issued digital currencies / J. Barrdear, M. Kumhof. – 2019. – 92 p. – URL: https://www.bis.org/events/confresearchnetwork1909/kumhof.pdf (date of access: 28.12.2021).

625. Bordo, M. Central Bank Digital Currency and the Future of Monetary Policy / M. Bordo, A. Levin // NBER Working Paper. – 2017. – No. 23711. – 32 p. – URL: https://www.nber.org/system/files/working_papers/w23711/w23711.pdf (date of access: 24.10.2019).

626. Bindseil U. Tiered CBDC and the financial system: European Central Bank / U. Bindseil // Working Paper Series. – 2020. – No 2351. – 41 p. – URL: https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp2351~c8c18bbd60.en.pdf (date of access: 27.08.2021).

627. Ткачёв, И. Налоговики запустят новые платформы для банков и чиновников / И. Ткачёв, Ю. Кошкина, А. Гальчева // РБК. – 2021. Режим доступа: https://www.rbc.ru/economics/04/03/2021/603f8ec99a7947c24dfd973a (дата обращения: 02.03.2022).

628. The future of cross-border payments. Evolution or revolution? OMFIF Digital Monetary Institute. – 2021. – 76 p. – URL: https://www.omfif.org/wp-content/uploads/2021/12/OMFIF_Future_of_Payments_2021.pdf (date of access: 19.01.2022).

629. К 2030 году три государства запустят свои токены. – 2020. – Режим доступа: https://whattonews.ru/k-2030-godu-tri-gosudarstva-zapustjat-svoi-tokeny/ (дата обращения: 27.08.2021).

630. К 2030 году 3–5 стран заменят фиат на CBDC. – 2020. – Режим доступа: https://whattonews.ru/k-2030-godu-3-5-stran-zamenjat-fiat-na-cbdc/ (дата обращения: 02.03.2022).

631. G20 Rome Leaders' Declaration. G20. – Italy, 2021. – URL: https://www.g20.org/wp-content/uploads/2021/10/G20-ROME-LEADERS-DECLARATION.pdf (date of access: 11.11.2021).

632. Major Eurozone banks start the implementation phase of a new unified payment scheme and solution, the European Payment Initiative (EPI). – 2020. – URL: https://www.bbva.com/en/major-eurozone-banks-start-the-implementation-phase-of-a-new-unified-payment-scheme-and-solution-the-european-payment-initiative-epi/ (date of access: 04.09.2020).

633. Open Banking: Is the Clock Ticking for European Banks? / Morgan Stanley. – 2021. – URL: https://www.morganstanley.com/ideas/open-banking-future-european-banks?subscribed=true&dis=em_2021317_wm_5ideasarticle&et_mid=227040&et_mkid= 12/03/2021 (date of access: 15.03.2021).

634. Qiu, T. Ripple vs. SWIFT: Transforming Cross Border. Remittance Using Blockchain Technology / T. Qiu, R. Zhang, Y. Gao // Procedia Computer Science. – 2019. – Vol. 147. – P. 428–434. – DOI: 10.1016/j.procs.2019.01.260.

635. Исследование: бизнес выбирает банки по цифровым сервисам: Пресс-релиз Райффайзенбанка. – 2021. – Режим доступа: https://www.raiffeisen.ru/about/press/releases/199080/ (дата обращения: 30.10.2021).

636. Фомин, Д. Сбербанк сообщил о планах запустить сервис для покупки цифровых активов / Д. Фомин // РБК. – 2020. – Режим доступа: www.rbc.ru/crypto/news/5fc502b29a794728d3689fe3 (дата обращения: 01.12.2020).

637. Трифонова, П. Билеты улетят за токены / П. Трифонова // Коммерсантъ. – № 153. – 2020. – С. 6. – Режим доступа: https://www.kommersant.ru/doc/4467224 (дата обращения: 28.08.2020).

638. Manikandan, A. ICICI, Kotak, Axis among 11 to launch Blockchain-linked funding for SMEs / A. Manikandan // Economic Times. – 2019. – URL: https://economictimes.indiatimes.com/markets/stocks/news/icici-kotak-axis-among-11-to-launch-blockchain-linked-funding-for-smes/articleshow/67718025.cms (date of access: 01.02.2020).

639. Галунов, А. Старейший банк Америки начнет работать с Bitcoin и другими криптовалютами / А. Галунов. – 2021. – Режим доступа: https://bloomchain.ru/newsfeed/stareishii-bank-ameriki-nachnet-rabotat-s-bitcoin-i-drugimi-kriptovaljutami?utm_source=telegram&utm_medium=social&utm_campaign=starejshij-bank-amer (дата обращения: 15.02.2021).

640. Ahmed, S. A Study on Trust Restoration Efforts in the UK Retail Banking Industry / S. Ahmed, K. Bangassa, S. Akbar // The British Accounting Review. – 2019. – Vol. 52 (1). – 42 p. – DOI: 10.1016/j.bar.2019.100871.

641. McWaters, J. The future of financial infrastructure, in: World Economic Forum: Deloitte Consulting LLP / J. McWaters. – 2016. – 130 p. – URL: https://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf (date of access: 20.05.2021).

642. Ikeda, K. Applications of Blockchain in the Financial Sector and a Peer-to-Peer Global Barter Web / K. Ikeda, M-N. Hamid // Advances in Computers. – 2018. – P. 99–120. – DOI: 10.1016/bs.adcom.2018.03.008.

643. Perez, Y. Santander: Blockchain TechCan Save Banks $20 Billion a Year / Y. Perez. – 2015. – URL: https://www.coindesk.com/business/2015/06/16/santander-blockchain-tech-can-save-banks-20-billion-a-year/ (date of access: 16.06.2015).

644. Irrera, A. Blockchain Could Save Investment Banks Up to $12 Billion a Year: Accenture / A. Irrera, J. Kelly. – 2017. – URL: https://www.reuters.com/article/us-banks-Blockchain-accenture/Blockchain-could-save-investment-banks-up-to-12-billion-a-year-accenture-idUSKBN1511OU (date of access: 20.02.2019).

645. Banking on Blockchain – A Value Analysis / Accenture Consulting. – 2017. – 10 p. – URL: https://www.accenture.com/t20170120T074124Z__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Consulting/Accenture-Banking-on-Blockchain.pdf#zoom=50 (date of access: 01.06.2021).

646. Del Castillo, M. Currency Settlement Service CLS Reveals Big Blockchain Ambitions / M. del Castillo. – 2016. – URL: https://www.coindesk.com/cls-to-develop-Blockchain-payment-service-on-ibm-fabric/ (date of access: 26.07.2019).

647. Xinghui, K. Singapore’s DBS bank to launch digital currency exchange featuring Bitcoin, Ether, XRP and Bitcoin cash / K. Xinghui. – 2020. – URL: https://www.scmp.com/week-asia/economics/article/3113409/singapores-dbs-bank-launch-digital-currency-exchange-featuring (date of access: 15.12.2020).

648. Q4 2020 DeFi Report / ConsenSys Codefi. – 2021. – 44 p. – URL: https://consensys.net/insights/q4-2020-defi-report/ (date of access: 13.05.2021).

649. Давыденко, Е. J P Morgan, HSBC, DBS: какие мировые банки использует блокчейн, и какие возможности перед ними открываются / Е. Давыденко. – 2021. – Режим доступа: https://psm7.com/blockchain/jp-morgan-hsbc-dbs-kakie-mirovye-banki-ispolzuyut-blokchejn-i-kakie-problemy-reshayut.html (дата обращения: 07.09.2021).

650. Top 10 trends in banking in 2016 / Capgemini. – 2016. – 26 p. – URL: https://www.capgemini.com/resources/banking-top-10-trends-2016/ (date of access: 27.02.2020).

651. Big data: the management revolution / A. McAfee [et al.] // Harvard Business Review. – 2012. – Vol. 90. – P. 60–68.

652. Moro, S. Business intelligence in banking: a literature analysis from 2002 to 2013 using text mining and latent Dirichlet allocation / S. Moro, P. Cortez, P. Rita // Expert Systems with Applications. – 2015. – Vol. 42. – P. 1314–1324.

653. Hirt, M. Strategic principles for competing in the digital age / M. Hirt, P. Willmott // McKinsey Quarterly. – 2014. – P. 1–13.

654. Strategic partnerships for the digital age // A Telstra report by The Economist Intelligence Unit. – 2015. – 48 p. – URL: http://connectedfuture.economist.com/wp-content/uploads/2016/10/Connecting-Companies-Whitepaper_final.pdf.pdf (date of access: 04.09.2019).

655. Криштаносов, В. Б. Современная цифровая финансовая инфраструктура: проблемы и перспективы развития / В. Б. Криштаносов // Экономика и управление производством: материалы докл. 85-й науч.-техн. конф. проф.-препод. состава, науч. сотрудников и аспирантов (с междунар. участием), Минск, 1–13 февраля 2021 г. / Бел. гос. технол. ун-т. – Минск: БГТУ, 2021. – С. 35–37.

656. Левочкина, А. От цифровых менеджеров до цифровых киллеров: что будет с финтехом в 2023 году / А. Левочкина. – 2021. – Режим доступа: https://frankrg.com/50552 (дата обращения: 10.10.2021).

657. Кошкина, Ю. Банки увидели конфликт интересов в антиотмывочном «светофоре» от ЦБ / Ю. Кошкина // РБК. – 2021. – Режим доступа: https://www.rbc.ru/finances/15/03/2021/604b86ec9a79473c3a38de2c (дата обращения: 17.03.2021).

658. Goode, A. Biometrics for banking best practices and barriers to adoption / A. Goode // Biometric Technology Today. – 2018. – Vol. 10. – P. 5–7. – DOI: 10.1016/S0969-4765(18)30156-5.

659. Asset Management as a Digital Platform Industry: A Global Financial Network Perspective / D. Haberly [et al.] // Geoforum. – 2019. – Vol. 106. – P. 167–181. – DOI: 10.1016/j.geoforum.2019.08.009.

660. Mooney, A. BlackRock Bets on Aladdin as Genie of Growth / A. Mooney // Financial Times. – 2017. – URL: https://www.ft.com/content/eda44658-3592-11e7-99bd-13beb0903fa3 (date of access: 31.05.2017).

661. Kaya, O. Robo-advice - a true innovation in asset management / O. Kaya // EU Monitor Global Financial Markets: Deutsche Bank Research. – 2017. – 16 p. – URL: https://www.dbresearch.com/PROD/RPS_ENPROD/PROD0000000000449125/Roboadvice_%E2%88%93_a_true_innovation_in_asset_managemen.pdf?undefined&realload=APRCaepkakDcrkPiaGacd1i4W6mHPVpVwyBE/uXMwk8DWE7AYEVyMP6j80FVK3IL (date of access: 15.08.2019).

662. Mason, T. U.S. Digital Adviser Forecast: AUM To Surpass $450B by 2021: S&P Global Market Intelligence / T. Mason. – 2017. – URL: https://www.spglobal.com/en/research-insights/articles/us-digital-adviser-forecast-aum-to-surpass-450b-by-2021 (date of access: 06.08.2019).

663. Haberly, D. Earth incorporated: centralization and variegation in the global company network / D. Haberly, D. Wojcik // Economic Geography. – 2017. – Vol. 93 (3). – P. 241–266.

664. Fichtner, J. Hidden power of the Big Three? Passive index funds, re-concentration of corporate ownership, and new financial risk / J. Fichtner, E. Heemskerk, J. Garcia-Bernardo // Business and Politics. – 2017. – Vol. 19 (2). – P. 298–326.

665. Bhaskar, N. Bitcoin Exchanges / N. Bhaskar, D. Lee, K. Chuen // Handbook of Digital Currency. – Cambridge: Elsevier Inc., 2015. – P. 559–573.

666. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system / S. Nakamoto. – 2008. – 11 p. – URL: https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf (date of access: 31.01.2019).

667. Turkay, B. An Evaluation of New Values in Economy and Their Impacts on Future Transformation in Tourism / B. Turkay, F. Dincer, M. Dincer // Procedia Computer Science. – 2019. – Vol. 158. – P. 1095–1102.

668. Isellioglu, C. An Investigation on the Volatility of Cryptocurrencies by means of Heterogeneous Panel Data Analysis / C. Isellioglu, S. Oner // Procedia Computer Science. – 2019. – Vol. 158. – P. 913–920.

669. Brito, J. Bitcoin: A Primer for Policymakers / J. Brito, A. Castillo; Mercatus Center: George Mason University. – 2013. – 48 p. – URL: http://mercatus.org/sites/default/files/Brito_BitcoinPrimer.pdf (date of access: 04.09.2019).

670. Lim, J. A Facilitative Model for Cryptocurrency Regulation in Singapore / J. Lim // Handbook of Digital Currency Bitcoin, Innovation, Financial Instruments, and Big Data. – 2015. – Chapter 18. – P. 361–381.

671. Sovbetov, Y. Factors influencing cryptocurrency prices: Evidence from Bitcoin, Ethereum, Dash, Litcoin, and Monero / Y. Sovbetov // Journal of Economics and Financial Analysis. – 2018. – Vol. 2 (2). – P. 1–2.

672. Nian, L. Introduction to Bitcoin / L. Nian, D. Lee, K. Chuen // Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data. – Cambridge: Elsevier Inc., 2015. – P. 6–30.

673. Knowledge Discovery in Cryptocurrency Transactions: A Survey / X. Liua [et al.]. – Cambridge: Elsevier Inc., 2020. – 60 p. – URL: https://arxiv.org/pdf/2010.01031.pdf (date of access: 10.10.2020).

674. Bitcoin mining pools: A cooperative game theoretic analysis / Y. Lewenberg [et al.] // Proceedings of the 14th International

Conference on Autonomous Agents and Multiagent Systems, AAMAS '15. – Citeseer, 2015. – P. 919–927.

675. Ren, L. Pooled mining is driving Blockchains toward centralized systems / L. Ren, P. Ward // 38th International Symposium on Reliable Distributed Systems Workshops. – 2019. – P. 43–48. – DOI:10.1109/Srdsw49218.2019.00015.

676. Wang, C. Measurement and analysis of the Bitcoin networks: A view from mining poolsar / C. Wang, X. Chu, Q. Yang // Proceedings 6th International Conference on Big Data Computing and Communications, BigCom. – Deqing, China, 2020. – P. 180–188. – DOI: 10.1109/BigCom51056.2020.00032.

677. Kristoufek, L. Bitcoin and its mining on the equilibrium path / L. Kristoufek // Energy Economics. – 2020. – Vol. 85 (C). – 21 p. – DOI: 10.1016/j.eneco.2019.104588.

678. Ammous, S. Can cryptocurrencies fulfil the functions of money? / S. Ammous // Quarterly Review of Economics and Finance. – 2018. – 55 p. – DOI: 10.1016Zj.qref.2018.05.010.

679. Katsiampa, P. An empirical investigation of volatility dynamics in the cryptocurrency market / P. Katsiampa // Research in International Business and Finance. – 2019. – Vol. 50. – P. 322–335. – DOI: 10.1016/j.ribaf.2019.06.004.

680. Yermack, D. Is Bitcoin a real currency? An economic appraisal / D. Yermack // Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments and Big Data. – Cambridge: Elsevier, 2015. – P. 31–44.

681. Cryptocurrencies as a Financial Asset: A systematic analysis. FINANA / S. Corbet [et al.]. – 2018. – 51 p. – DOI: 10.1016/j.irfa.2018.09.003.

682. Bitcoin for energy commodities before and after the December 2013 crash: diversifier, hedge or safe haven? / E. Bouri [et al.] // Applied Economics. – 2017. – Vol. 49 (50). – P. 5063–5073.

683. Baur, D. Bitcoin: Medium of Exchange or Speculative Assets? / D. Baur, K. Hong, A. Lee // Journal of International Financial Markets, Institutions & Money. – 2017. – Vol. 54. – P. 177–189. – DOI: 10.1016/j.intfin. 2017.12.004.

684. Lee, D. Cryptocurrency: a new investment opportunity? / D. Lee, L. Guo, Y. Wang // The Journal of Alternative Investments. – 2018. – Vol. 20 (3). – P. 16–40.

685. Cryptocurrencies as a Financial Asset: A systematic analysis / S. Corbet [et al.] // International Review of Financial Analysis. – 2018. – Vol. 62 (C). – P. 182–199. – DOI: 10.1016/j.irfa.2018.09.003.

686. Hileman, G. A History of Alternative Currencies / G. Hileman. – London: London School of Economics, 2014. – 31 p. – URL: https://www.hillsdale.edu/wp-content/uploads/2016/02/FMF-2014-A-History-of-Alternative-Currencies.pdf (date of access: 28.01.2021).

687. Tasca, P. Taxonomy of blockchain technologies / P. Tasca, C. Tessone // Principles of identifcation and classifcation. – 2018. – 43 p. – DOI: 10.2139/ssrn.2977811.

688. Bitcoin Returns and Risk: A General GARCH and GAS Analysis / V. Troster [et al.] // Finance Research Letters. – 2018. – Vol. 30 (C). – P. 187–193. – DOI: 10.1016/j.frl.2018.09.014.

689. Baek, C. Bitcoins as an investment or speculative vehicle? A first look / C. Baek, M. Elbeck // Applied Economics Letters. – 2015. – Vol. 22. – P. 30–34.

690. Does Bitcoin hedge global uncertainty? Evidence from wavelet-based quantile-in-quantile regressions / E. Bouri [et al.] // Finance Research Letters. – 2017. – Vol. 23. – P. 87–95.

691. An introduction to Blockchain, cryptocurrency and Initial Coin Offerings / P. Martino [et al.] // New Frontiers in Entrepreneurial Finance Research. – Singapore: World Scientific Publishing Co., 2019. – Chapter 7. – P. 181–206.

692. Chen, Y. Blockchain disruption and decentralized finance: The rise of decentralized business models / Y. Chen, C. Bellavitis // Journal of Business Venturing Insights. – 2020. – Vol. 13. – 8 p. – URL: https://www.researchgate.net/publication/337111343_Blockchain_Disruption_and_Decentralized_Finance_The_Rise_of_Decentralized_Business_Models. DOI: 10.1016/j.jbvi.2019.e00151 (date of access: 23.12.2020).

693. Adhami, S. Why do business go crypto? An empirical analysis of initial coin offering: SSRN / S. Adhami, G. Giudici, S. Martinazzi. – 2017. – 36 p. – URL: https://www.researchgate.net/publication/320161179_Why_do_businesses_go_crypto_An_empirical_analysis_of_Initial_Coin_Offerings (date of access: 13.03.2019).

694. Fisch, C. Initial coin offerings (ICOs) to finance new ventures / C. Fisch // Journal of Business Venturing. – 2019. – Vol. 34. – P. 1–22. DOI: 10.1016/j.jbusvent.2018.09.007.

695. Sameeh, T. ICO Basics – Security Tokens vs. Utility Tokens / T. Sameeh. – 2018. – URL: https://www.cointelligence.com/content/ico-basics-security-tokens-vs-utility-tokens/ (date of access: 01.04.2020).

696. Motives and profiles of ICO investors / C. Fisch [et al.] // Journal of Business Research. – 2019. – Vol. 125 (C). – P. 564–576. – DOI: 10.1016/j.jbusres.2019.07.036.

697. Kaal, W. Initial coin offerings: the top 25 jurisdictions and their comparative regulatory responses / W. Kaal // SSRN Electronic Journal. – 2018. – 29 p. – DOI: 10.2139/ssrn.3117224.

698. Отчет за 2-й квартал 2020 г. // Bloomchain.ru. – 2020. – 33 с. – Режим доступа: https://bloomchain-cdn.s3.amazonaws.com/uploads/pdf/394c0200-d0de-11ea-adbe-0242ac130003/original.pdf?v=63763165545 (дата обращения: 29.07.2021).

699. Roth, N. An Architectural Assessment of Bitcoin. Using the Systems Modeling Language / N. Roth // Procedia Computer Science. – 2015. – Vol. 44. – P. 527–536. – DOI: 10.1016/j.procs.2015.03.066.

700. Tasca, P. The dual nature of Bitcoin as payment network and money / P. Tasca // SUERF Conference Proceedings. – 2016. – VI Chapter. – URL: https://ssrn.com/abstract=2805003 (date of access: 16.08.2019).

701. Wood, G. Ethereum: A secure decentralized generalized transaction ledger eip-150 revision / G. Wood. – 2017. – 41 p. – URL: https://ethereum.github.io/yellowpaper/paper.pdf (date of access: 29.07.2020).

702. Smart contracts in financial services: Getting from hype to reality / Capgemini Consulting / B. Cant [et al.]. – 2016. – P. 1–26. – URL: https://www.capgemini.com/consulting-de/wp-content/uploads/sites/32/2017/08/smart_contracts_ paper_long_0.pdf (date of access: 13.03.2019).

703. Tapscott, A. How Blockchain is changing finance / A. Tapscott, D. Tapscott // Harvard Business Review. – 2017. – Vol. 1. – URL: https://hbr.org/2017/03/how-blockchain-is-changing-finance (date of access: 29.07.2020).

704. Ante, L. The Influence of Stablecoin Issuances on Cryptocurrency Markets / L. Ante, I. Fiedler, E. Strehle // Finance Research Letters. – 2021. – Vol. 41. – 15 p. – DOI: 10.1016/j.frl.2020.101867.

705. Moin, A. SoK: A Classification Framework for Stablecoin Designs. Financial Cryptography and Data Security / A. Moin, K. Sekniqi, E. Sirer // 24th International Conference, FC 2020. – Kota Kinabalu, Malaysia, February 10–14, 2020. – P. 174–197.

706. Sidorenko, E. Stablecoin as a New Financial Instrument / E. Sidorenko // Digital Age: Chances, Challenges and Future. – 2019. – Vol. 84. – P. 630–638. – DOI: 10.1007/978-3-030-27015-5_75.

707. Годовой отчет за 2020 год // CoinGecko. – 2020. – 39 p. – Режим доступа: https://assets.coingecko.com/reports/2020-Year-End-Report/CoinGecko-2020-Report.pdf (дата обращения: 28.05.2021).

708. Meyer, D. More Banks Are Trying Out Blockchains for Fund Transfers / D. Meyer // Fortune. – 2016. – URL: https://fortune.com/2016/06/23/ripple-blockchain-banks/ (date of access: 17.12.2019).

709. Фомин, Д. За последний месяц DeFi-токены подорожали на 500–1000%. Что это такое? / Д. Фомин // РБК. – 2020. – Режим доступа: https://www.rbc.ru/crypto/news/5f2e845a9a7947478992bbe9 (дата обращения: 16.09.2021).

710. Ключевые тренды на рынке криптовалют и DeFi 4Q 2020 // Bloomchain. – 2021. – Режим доступа: https://bloomchain-cdn.s3.amazonaws.com/uploads/pdf/dacc7404-661e-11eb-9358-0242ac130003/original.pdf?v=63779576027 (дата обращения: 03.02.2022).

711. Sebastião, H. Bitcoin futures: An effective tool for hedging cryptocurrencies / H. Sebastião, P. Godinho // Finance Research Letters. – 2020. – Vol. 33 (C). – 6 p. – DOI: 10.1016/j.frl.2019.07.003.

712. Первый день торгов фьючерсами на ETH показал очень хорошие результаты. – 2021. – Режим доступа: https://whattonews.ru/pervyj-den-torgov-fjuchersami-na-eth-pokazal-ochen-horoshie-rezultaty/ (дата обращения: 10.02.2021).

713. Танзил, А. Есть ли спрос на производные инструменты на основе биткоина? / А. Танзил // investing.com. – 2019. – Режим доступа: https://ru.investing.com/analysis/article-200260449 (дата обращения: 30.12.2020).

714. Анащенков, Ф. Как запуск криптоиндексов от S&P Dow Jones изменит биткоин-индустрию / Ф. Анащенков // forklog.com. – 2020. – Режим доступа: https://forklog.com/kak-zapusk-kriptoindeksov-ot-s-p-dow-jones-izmenit-bitkoin-industriyu/ (дата обращения: 16.09.2021).

715. Coursey, D. Models of e-government: are they correct? An empirical assessment / D. Coursey, D. Norris // Public Administration Review. – 2008. – Vol. 68. – P. 523–536. – DOI:10.1111/j.1540-6210.2008.00888.x.

716. Ojo, A. Government 3.0 – next generation government technology infrastructure and services: Roadmaps, enabling technologies & challenges / A. Ojo, J. Millard. – London: Springer, 2017. – 363 p. – DOI: 10.1007/978-3-319-63743-3.

717. Federal Reserve Policy on Payment System Risk: Federal Reserve. – 2021. – 36 p. – URL: https://www.federalreserve.gov/paymentsystems/files/psr_policy.pdf (date of access: 03.02.2022).

718. Klievink, B. Realizing joined-up government – Dynamic capabilities and stage models for transformation / B. Klievink, M. Janssen // Government Information Quarterly. – 2009. – Vol. 26 (2). – P. 275–284. – DOI: 10.1016/j.giq.2008.12.007.

719. The E-Government Handbook for Developing Countries / World-Bank. E-Gov Guideline. – 2002. – 41 p. – URL: https://documents1.worldbank.org/curated/en/317081468164642250/pdf/320450egovhandbook01public12002111114.pdf (date of access: 24.10.2019).

720. Zeleti, F. Critical factors for dynamic capabilities in open government data enabled organizations / F. Zeleti, A. Ojo // Proceedings of the 17th international digital government research conference on digital government research. – 2016. – P. 86–96. – DOI: 10.1145/2912160.2912164.

721. Anthopoulos L. Smart government: A new adjective to government transformation or a trick? Understanding smart cities: A tool for smart government or an industrial trick? / L. Anthopoulos. – London: Springer Int., 2017. – P. 263–293.

722. Gil-Garcia, J. Conceptualizing smartness in government: An integrative and multi-dimensional view / J. Gil-Garcia, J. Zhang, G. Puron-Cid // Government Information Quarterly. – 2016. – Vol. 33 (3). – P. 524–534.

723. Bertot, J. Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies / J. Bertot, P. Jaeger, J. Grimes // Government Information Quarterly. – 2010. – Vol. 27 (3). – P. 264–271.

724. Eggers, W. AI augmented government: using cognitive technologies to redesign public sector work: Deloitte Center for Government Insights / W. Eggers, D. Schatsky, P. Viechnicki. – 2017. – 24 p. – URL: https://www2.deloitte.com/content/dam/insights/us/articles/3832_AI-augmented-government/DUP_AI-augmented-government.pdf (date of access: 07.05.2020).

725. Wirtz, B. Artificial intelligence and the public Sector – Applications and challenges / B. Wirtz, J. Weyerer, C. Geyer // International Journal of Public Administration. – 2019. – Vol. 42 (7). – P. 596–615.

726. The Global Risks Report: World Economic Forum. – 2022. – URL: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf (date of access: 19.01.2022).

727. Ruan, K. Cyber Risk Management: A New Era of Enterprise Risk Management / K. Ruan // Digital Asset Valuation and Cyber Risk Measurement Principles of Cybernomics. – Cambridge: Elsevier Inc., 2019. – P. 49–73. – DOI: 10.1016/B978-0-12-812158-0.00003-X.

728. International Organization for Standardization (ISO). Risk Management – Principles and Guidelines: ISO 31000. – 2009. – URL: https://www.iso.org/iso-31000-risk-management.html (date of access: 11.04.2020).

729. Quality vocabulary. Availability, reliability, and maintainnability terms. Guide to concepts and related definitions. BS 4778-3.1:1991. – London: British Standards Institution, 1991. – 32 p.

730. International Risk Governance Council (IRGC). The Emergence of Risks. Contributing Factors. – Geneva, 2010. – URL: www.irgc.org (date of access: 10.02.2020).

731. International Risk Governance Council (IRGC). Improving the Management of Emerging Risks. – Geneva: IRGC, 2011. – URL: www.irgc.org (date of access: 10.02.2020).

732. Ramezani, J. Approaches for resilience and antifragility in collaborative business ecosystems / J. Ramezani, L. Camarinha-Matos // Technological Forecasting & Social Change. – 2020. – Vol. 151. – 26 p. – URL: https://doi.org/10.1016/j.techfore.2019.119846 (date of access: 15.04.2020).

733. Consumer-facing technology fraud: Economics, attack methods and potential solutions / M. Ali [et al.] // Future Generation Computer Systems. – 2019. – Vol. 100. – P. 408–427. – DOI: 10.1016/j.future.2019.03.041.

734. Sharafaldin, I. An evaluation framework for network security visualizations / I. Sharafaldin, A. Lashkari, A. Ghorbani // Computers & Security. – 2019. – Vol. 84. – P. 70–92. – DOI: 10.1016/j.cose.2019.03.005.

735. Choo, K-Kr. The cyber threat landscape: challenges and future research directions / K-Kr. Choo // Computers & Security. – Vol. 30 (8). – 2011. – P. 719–731.

736. Hunton, P. Data attack of the cybercriminal: Investigating the digital currency of cybercrime / P. Hunton // Computer Law & Security Review. – 2012. – Vol. 28. – P. 201–207. DOI: 10.1016/j.clsr.2012.01.007.

737. NIST. Guide for Conducting Risk Assessments. Special Publication 800–30 Rev 1: US Department of Commerce. – Washington D C, 2012. – 95 p. – URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf (date of access: 01.03.2020).

738. Financial stability implications from FinTech: Financial Stability Board. – 2017. – 65 p. – URL: http://www.fsb.org/wp-content/uploads/R270617.pdf (date of access: 02.03.2020).

739. Volz, D. Cyber attacks loom as growing corporation credit risk: Moody's / D. Volz. – 2015. – URL: http://www.reuters.com/article/us-cybersecurity-moody-s-idUSKBN0TC2CP20151123 (date of access: 02.04.2020).

740. Goolsbee, A. Public policy in an AI economy / A. Goolsbee; National bureau of economic research: Working Paper. – May 2018. –

No. 24653 – 11 p. – URL: http://www.nber.org/papers/w24653.parliament.uk/pa/cm201617/cmselect/cmsctech/270/270.pdf (date of access: 15.01.2019).

741. Towards an Integrative Approach. International Risk Governance Council (IRGC). White Paper on Risk Governance. – Geneva, 2005. – URL: www.irgc.org (date of access: 04.06.2020).

742. Boyson, S. Cyber supply chain risk management: Revolutionizing the strategic control of critical it systems / S. Boyson // Technovation. – 2014. – Vol. 34 (7). – P. 342–353.

743. Tomlin, B. On the value of mitigation and contingency strategies for managing supply chain disruption risks / B. Tomlin // Management Science. – 2006. – Vol. 52 (5). – P. 639–657. – DOI: 10.1287/mnsc.1060.0515.

744. Gerber, M. Management of risk in the information age / M. Gerber, R. von Solms // Computer Security. – 2005. – Vol. 24. – P. 16–30.

745. Lacon, M. Risk Assessment and Monitoring in Intelligent Data-Centric Systems / M. Lacon, S. Marron // Security and Resilience in Intelligent Data-Centric Systems and Communication Networks. – Cambridge: Elsevier Inc., 2018. – P. 29–52. – DOI: 10.1016/B978-0-12-811373-8.00002-1.

746. Fischer, R. Risk Analysis, Security Surveys and Insurance / R. Fischer, E. Halibozek, D. Walters // Introduction to Security. – Cambridge: Elsevier Inc., 2019. – P. 137–168. – DOI: 10.1016/B978-0-12-805310-2.00007-X.

747. Nauck, F. The disaster you could have stopped: Preparing for extraordinary risks / F. Nauck, O. Usher, L. Weiss; McKinsey&Company, 2020. – 9 p. – URL: https://www.mckinsey.com/business-functions/risk/our-insights/the-disaster-you-could-have-stopped-preparing-for-extraordinary-risks?cid=other-eml-nsl-mip-mck&hlkid=061d027268294196b455863b2fa7bbd6&hctky=11708326&hdpid=89044107-4811-4e7a-a384-9ca7c398bac6 (date of access: 13.03.2020).

748. Aminzade, M. Confidentiality, integrity and availability – finding a balanced IT framework / M. Aminzade // Network Security. – 2018. – No. 5. – P. 9–11. – DOI: 10.1016/S1353-4858(18)30043-6.

749. Security and Privacy Controls for Federal Information Systems and Organizations. NIST Special Publication 800-53 / National Institute of Standards and Technology. – 2020. – 492 p. – URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (date of access: 13.03.2021).

750. Introduction to Threat Modeling: Microsoft. – 2020. – 77 p. – URL: https://download.microsoft.com/download/9/3/5/935520EC-D9E2-413E-BEA7-0B865A79B18C/Introduction_to_Threat_Modeling.ppsx (date of access: 10.01.2020).

751. What is the CIA Triad? – 2019. – URL: https://www.forcepoint.com/cyber-edu/cia-triad (date of access: 21.10.2021).

752. Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience: World Economic Forum. – Cologny, Switzerland, 2012. – 48 p. – URL: https:// https://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf (date of access: 09.02.2019).

753. Cavusoglu, H. The effect of Internet security breach announcements on market value of breached firms and Internet security developers / H. Cavusoglu, B. Mishra, S. Raghunathan // International Journal of Electronic Commerce. – 2004. – Vol. 9 (1). – P. 69–104.

754. Emerging Systemic Risks in the 21st Century: An Agenda for Action. Paris: Organization for Economic Co-Operation and Development (OECD). – 2003. – URL: http://www.oecd.org/ (date of access: 08.14.2019).

755. Managing emerging technology-related risks. Standard Recommendation. S.R. CWA 16649. – 2013. – URL: https://shop.standards.ie/preview/98705249998.pdf?sku=877230_SAIG_NSAI_ NSAI_2084853 (date of access: 01.28.2019).

756. Ellwood, P. Green Jobs and Occupational Safety and Health: Foresight on New and Emerging Risks Associated with New Technologies by 2020 / P. Ellwood, J. Reynolds, M. Duckworth // EU-OSHA (European Agency for Safety and Health at Work). – Luxembourg, 2014. – URL: http://osha.europa.eu (date of access: 23.07.2019).

757. Ruan, K. Cyber Risk Measurement in the Hyperconnected World / K. Ruan // Digital Asset Valuation and Cyber Risk Measurement Principles of Cybernomics. – Cambridge: Elsevier Inc., 2019. – P. 75–86. – DOI: 10.1016/B978-0-12-812158-0.00004-1.

758. Huq, N. TrendLabs Research. Follow the Data: Dissecting Data Breaches and Debunking Myths / N. Huq // Trend Micro Analysis of Privacy Rights Clearinghouse 2005–2015. Data Breach Records. – Tokyo, Japan: Trend Micro, 2015. – 51 p. – URL: https://documents.trendmicro.com/assets/wp/wp-follow-the-data.pdf (date of access: 04.05.2021).

759. Pursiainen, C. Critical infrastructure resilience: A Nordic model in the making? / C. Pursiainen // International Journal of Disaster Risk Reduction. – 2018. – Vol. 27. – P. 632–641. – DOI: 10.1016/j.ijdrr.2017.08.006.

760. McClure, S. Hacking exposed: Network security secrets and solutions / S. McClure, J. Scambray, G. Kurtz. – Berkeley, Calif: Osborne: McGraw-Hill, 2001. – 1086 p. – URL: https://doc.lagout.org/security/Hacking%20Exposed.pdf (date of access: 21.10.2021).

761. A literature review on Smart Cities: paradigms, opportunities and open problems / A. Arroub [et al.] // International Conference on Wireless Networks and Mobile Communications (WINCOM), IEEE. – 2016. – P. 180–186.

762. Palanisamy, B. Security and privacy issues in E-Government / B. Palanisamy // E-Government Service Maturity and Development: Cultural, Organizational and Technological Perspectives. – Hershey: IGI Global. – 2012. – P. 236–248.

763. Zhao, J. Opportunities and threats: a security assessment of state e-government websites / J. Zhao, S. Zhao // Government Information Quarterly. – 2010. – Vol. 27 (1). – P. 49–56.

764. Ummelas, O. Clients of Estonia's E-Residency Project Linked to Crypto Scams / O. Ummelas. – 2020. – URL: https://archive.is/ddecx#selection-2447.0-2447.18 (date of access: 09.02.2021).

765. Литова, Е. После внедрения цифрового рубля из банков может утечь 9 трлн рублей / Е. Литова, С. Шелудченко // Ведомости. – 2021. – Режим доступа: https://www.vedomosti.ru/finance/articles/2021/11/01/893920-iz-bankov-posle-vnedreniya-tsifrovogo-rublya-mozhet-utech-9-trln (дата обращения: 11.11.2021).

766. Банки опасаются внедрения цифрового рубля. – 2021. – Режим доступа: https://whattonews.ru/banki-opasajutsja-vnedrenija-cifrovogo-rublja/ (дата обращения: 15.01.2021).

767. Казарновский, П. Эксперты назвали главные риски внедрения цифрового рубля в России / П. Казарновский, Ю. Кошкина. – 2021. – Режим доступа: https://www.rbc.ru/finances/12/01/2021/5ffc4caf9a79470d03a85b55 (дата обращения: 15.01.2021).

768. Bitcoin price growth and Indonesia's monetary system / P. Narayan [et al.] // Emerging Markets Review. – 2018. – Vol. 38 (C). – P. 364–376. – DOI: 10.1016/j.ememar.2018.11.005.

769. Xiong, J. A New Method to Verify Bitcoin Bubbles: Based on the Production Cost / J. Xiong, Q. Liu, L. Zhao // North American Journal of Economics & Finance. – 2020. – Vol. 51 (7). – 17 p. – DOI: 10.1016/j.najef. 2019.101095.

770. FCA warns consumers of the risks of investments advertising high returns based on cryptoassets. – 2021. – URL: https://www.fca.

org.uk/news/news-stories/fca-warns-consumers-risks-investments-advertising-high-returns-based-cryptoassets (date of access: 12.02.2021).

771. Kharpal, A. Report finds $50 billion of cryptocurrency moved out of China hinting at capital flight against Beijing rules / A. Kharpal. – 2021. – URL: https://www.cnbc.com/2020/08/21/china-users-move-50-billion-of-cryptocurrency-out-of-country-hinting-at-capital-flight.html (date of access: 25.05.2022).

772. Банки не могут идентифицировать до 90% подозрительных криптосделок. – 2020. – Режим доступа: https://coinspot.io/cryptocurrencies/banki-ne-mogut-identificirovat-do-90-podozritelnyh-kriptosdelok/ (дата обращения: 15.09.2020).

773. An efficient linkable group signature for payer tracing in anonymous q cryptocurrencies / L. Zhang [et al.] // Future Generation Computer Systems. – 2019. – Vol. 101. – P. 29–38. – DOI: 10.1016/j.future.2019.05.081.

774. Toward privacy and regulation in blockchain-based cryptocurrencies / Y. Li [et al.] // IEEE Network. – 2019. – Vol. 33 (5). – P. 111–117. – DOI: 10.1109/MNET.2019.1800271.

775. A geographical analysis of trafficking on a popular darknet market / J. Broseus [et al.] // Forensic Science International. – 2017. – Vol. 277. – P. 88–102. – DOI: 10.1016/j.forsciint.2017.05.021.

776. Acin, V. Making sense of the dark web / V. Acin // Computer Fraud & Security. – July 2019. – P. 17–19.

777. The 2020 Geography of Cryptocurrency Report. Analysis of Geographic Trends in Cryptocurrency Adoption, Usage, and Regulation // Chainalysis. – 2020. – 132 p. – URL: https://go.chainalysis.com/rs/503-FAP-074/images/2020-Geography-of-Crypto.pdf (date of access: 13.03.2021).

778. Carter, N. How Much Energy Does Bitcoin Actually Consume? / N. Carter // Harvard Business Review. – 2021. – URL: https://hbr.org/2021/05/how-much-energy-does-bitcoin-actually-consume (date of access: 07.05.2021).

779. Foley, S. Sex, drugs, and Bitcoin: how much illegal activity is financed through cryptocurrencies? / S. Foley, J. Karlsen, T. Putnins // The Review of Financial Studies. – 2019. – Vol. 32 (5). – P. 1798–1853.

780. Crypto Crime Report. 2020 // Chainalysis. – 2020. – URL: https://go.chainalysis.com/2020-CryptoCrime-Report.html (date of access: 14.04.2021).

781. Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets: Department of The Treasury Financial Crimes Enforcement Network 31 CFR Parts 1010, 1020, and 1022 RIN 1506-AB47 federalregister.gov/d/2020-28437 // Federal Register. – 2020. – Vol. 85. – No. 247. – URL: http://federalregister.gov/d/2020-28437.pdf (date of access: 04.01.2021).

782. Osborne, C. Russian dark web marketplace Hydra cryptocurrency transactions reached $1.37bn in 2020 / C. Osborne. – 2021. – URL: https://www.zdnet.com/article/russian-dark-web-marketplace-hydra-cryptocurrency-transactions-reached-1-37bn-in-2020/ (date of access: 03.02.2022).

783. Касперский, Е. Цифровой преступный мир самоизолировался, но не ушел на каникулы / Е. Касперский // Harvard Business Review. Россия. – 2021. – Режим доступа: https://hbr-russia.ru/innovatsii/tekhnologii/854790 (дата обращения: 01.04.2020).

784. Financial Inclusion: Can It Meet Multiple Macroeconomic Goals? / IMF, SDN/15/17. – September 2015. – 33 p. – URL: https://www.imf.org/external/pubs/ft/sdn/2015/sdn1517.pdf (date of access: 20.12.2019).

785. Su, T. Balancing Innovation and Risks in Digital Financial Inclusion – Experiences of Ant Financial Services Group / T. Su // Handbook of Blockchain, Digital Finance, and Inclusion. – 2018. – Vol. 2. – P. 37–43. – DOI: 10.1016/B978-0-12-812282-2.00002-4.

786. Entrenching Innovation / The 4th UK Alternative Finance Industry Report Cambridge Centre for Alternative Finance / B. Zheng [et al.]. – 2017. – 69 p. – URL: https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3084570_code2820904.pdf?abstractid=3084570&mirid=1 (date of access: 01.04.2019).

787. Hill, J. Bubbles, Panics, Crashes, and Crises / J. Hill // Fintech and the Remaking of Financial Institutions. – Cambridge: Elsevier, 2018. – P. 113–115. – DOI: 10.1016/B978-0-12-813497-9.00005-6.

788. Putilov, A. V. Development of Russian labor market in the context of informatization and computerization of the economy / A. V. Putilov, M. V. Bugaenko, D. V. Timokhin // Procedia Computer Science. – 2018. – Vol. 145. – P. 169– 176. – DOI: 10.1016/j.procs.2018.11.035.

789. Balsmeier, B. Is this time different? How digitalization influences job creation and destruction / B. Balsmeier, M. Woerter // Research Policy. – 2019. – Vol. 48 (8). – 10 p. – DOI: 10.1016/j.respol.2019.03.010.

790. Frey, C. The future of employment: how susceptible are jobs to computerization? / C. Frey, M. Osborne // Technological Forecasting and Social Change. – 2017. – Vol. 114. – P. 254–280.

791. The Future of Jobs: Report WEF. – October 2020. – 163 p. – URL: http://www3.weforum.org/docs/WEF_Future_of_Jobs_2020.pdf (date of access: 13.05.2021).

792. Richardson, L. Geographies of digital skill: Geoforum / L. Richardson, D. Bissell. – 2017. – 9 p. – URL: https://www.mckinsey.com/~/media/McKinsey/Global%20Themes/Future%20of %20Organizations/What %20the% 20future% 20of% 20work%20will% 20mean% 20for % 20iobs%20skills%20and%20wages/MGI-Jobs-Lost-Jobs-Gained-Report-December-6-2017.ashx> (date of access: 23.08.2019).

793. Goralski, M. Artificial intelligence and sustainable development / M. Goralski, T. Tarr // The International Journal of Management Education. – 2020. – Vol. 18 (1). – 9 p. – DOI:10.1016/j.ijme.2019.100330.

794. Aghion, P. Artificial Intelligence and Economic Growth: NBER Working Paper Series / P. Aghion, B. Jones, C. Jones // National Bureau of Economic Research. – October 2017. – No. 23928. – 56 p. – URL: http://www.nber.org/papers/w23928 (date of access: 07.08.2019).

795. Tirole, J. Economics for the Common Good / J. Tirole. – Princeton University Press, 2017. – 576 p. – URL: https://gdsnet.org/Tirole2019FrontMatterChapt1.pdf (date of access: 04.12.2018).

796. The Global Risks Report / WEF. – 2021. – 97 p. – URL: http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf (date of access: 03.02.2022).

797. Данильченко, А. В. Цифровая трансформация обрабатывающей промышленности Республики Беларусь: тенденции и перспективы развития / А. В. Данильченко, И. А. Зубрицкая, К. В. Якушенко; Бел. нац. ун-т. – Минск: Право и экономика, 2019. – 246 с.

798. Defossez, K. Seven steps to help protect your ERP system against cyberattacks: McKinsey Report / K. Defossez, W. Richter. – 2022. – 5 p. – URL: https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/seven%20steps%20to%20help%20protect%20your%20erp%20system%20against%20cyberattacks/seven-steps-to-help-protect-your-erp-system-against-cyberattacks.pdf?shouldIndex=false (date of access: 05.04.2022).

799. Mylrea, M. Smart energy-internet-of-things opportunities require smart treatment of legal, privacy and cybersecurity challenges /

M. Mylrea // Journal of World Energy Law and Business. – 2017. – Vol.10 (2). – P. 147–158.

800. Tweneboah-Koduah, S. Cybersecurity threats to IoT applications and service domains / S. Tweneboah-Koduah, K. Skouby, R. Tadayoni // Wireless Personal Communications. – 2017. – Vol. 95 (1). – P. 169–185. – DOI: 10.1007/s11277-017-4434-6.

801. Zeadally, S. Cryptographic technologies and protocol standards for internet of Things / S. Zeadally, A. Das, N. Sklavos // Internet of Things. – 2021. – Vol. 14. – 11 p. – DOI: 10.1016/j.iot.2019.100075.

802. Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches / M. Hasan [et al.] // Internet of Things. – 2019. – Vol 7. – 14 p. – DOI: 10.1016/j.iot.2019.100059.

803. Comprehending the IoT cyber threat landscape: A data dimensionality reduction technique to infer and characterize Internet-scale IoT probing campaigns / M. Pour [et al.] // Digital Investigation. – 2019. – Vol. 28. – P. 40–49. – DOI: 10.1016/j.diin.2019.01.014.

804. IoT architecture challenges and issues: Lack of standardization / S. Al-Qaseemi [et al.] // Proceedings of FTC 2016 – Future technologies conference. – United States, San Francisco, 2016. – P. 731–738.

805. Hogan, M. NIST interagency report (NISTIR) 8200, interagency report on status of international cybersecurity standardization for the Internet of Things (IoT) / M. Hogan, B. Piccarreta. – 2018. – 187 p. – URL: https://csrc.nist.gov/publications/detail/nistir/8200/draft (date of access: 20.02.2022).

806. Minoli, D. Blockchain mechanisms for IoT security / D. Minoli, B. Occhiogrosso // Internet of Things. – 2018. – Vol. 514-2. – P. 1–13. – DOI: 10.1016/j.iot.2018.05.002.

807. Tumpe, M. Investigating Security Issues in Cloud Computing / M. Tumpe, B. Jagdev // Complex, Intelligent and Software Intensive Systems (CISIS): Eighth International Conference IEEE. – Birmingham, 2014. – P. 141–146. – DOI: 10.1109/CISIS.2014.21.

808. PoRX: A reputation incentive scheme for blockchain consensus of IioT / E. Wang [et al.] // Future Generation Computer Systems. – 2020. – Vol. 102. – P. 140–151. – DOI: 10.1016/j.future.2019.08.005.

809. Estimating the impact of IT security incidents in digitized production environments / O. Burger [et al.] // Decision Support Systems. – 2019. – Vol. 127 (10). – 11 p. – DOI: 10.1016/j.dss.2019.113144.

810. Heritage, I. Protecting Industry 4.0: challenges and solutions as IT, OT and IP converge / I. Heritage // Network Security. – October, 2019. – P. 6–9. – DOI: 10.1016/S1353-4858(19)30120-5.

811. Asghar, M. Cybersecurity in industrial control systems: Issues, technologies, and challenges / M. Asghar, Q. Hu, S. Zeadally // Computer Networks. – 2019. – Vol. 165. – 16 p. – DOI: 10.1016/j.comnet.2019.106946.

812. The Power Grid: Smart, Secure, Green and Reliable / ed. B. D'Andrade. Cybersecurity for the smart grid / A. Sorini, E. Staroswiecki. – Cambridge: Elsevier, 2017. – Chapter 8. – P. 233–252. – DOI: 10.1016/B978-0-12-805321-8.00008-2.

813. Impact Of Cyber-Attacks On Critical Infrastructure / K. Thakur [et al.] // IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), High Performance and Smart Computing (HPSC) and Intelligent Data and Security (IDS). – New York, 2016. – P. 183–186. – DOI: 10.1109/BigDataSecurity-HPSC-IDS.2016.22.

814. Kimani, K. Cyber Security Challenges for IoT-based Smart Grid Networks / K. Kimani, V. Oduol, K. Langat // International Journal of Critical Infrastructure Protection. – 2019. – Vol. 25. – P. 36–49. – DOI: 10.1016/j.ijcip.2019.01.001.

815. Mansfield-Devine, S. Nation-state hacking threat to everyone / S. Mansfield-Devine // Computer Fraud & Security. – 2018. – P. 17–20. DOI: 10.1016/S1361-3723(18)30077-0.

816. Tariq, N. Securing SCADA-based Critical Infrastructures: Challenges and Open Issues / N. Tariq, M. Asim, F. Khan // Procedia Computer Science. – 2019. – Vol. 155. – P. 612–617. – DOI: 10.1016/j.procs.2019.08.086.

817. Townsend, A. Smart cities: Big data, civic hackers, and the quest for a new utopia / A. Townsend. – New York: WW Norton & Company, 2013. – 400 p.

818. Cryptocurrency anti-money laundering report Q4 2019 // CipherTrace. Cryptocurrency Intelligence. – 2019. – URL: https://ciphertrace.com/q4-2019-cryptocurrency-anti-money-laundering-report/ (date of access: 25.07.2020).

819. Falliere, N. W32.stuxnet / N. Falliere, L. Murchu, E. Chien. – 2011. – 69 p. – URL: https://archive.org/details/w32_stuxnet_dossier (date of access: 01.01.2020).

820. Communications Fraud Control Association (CFCA) Announces Results of Worldwide Telecom Fraud Survey. – 2016. – URL: https://goo.gl/H1VLae (date of access: 21.11.2021).

821. Число преступлений, связанных с криптовалютами, снизилось на 57%. – 2021. – Режим доступа: https://coinspot.io/analysis/

chislo-prestuplenij-svyazannyh-s-kriptovalyutami-snizilos-na-57/ (дата обращения: 18.08.2021).

822. Crypto Crime Report. – 2021. – URL: https://go.chainalysis.com/2021-Crypto-Crime-Report.html (date of access: 03.04.2021).

823. A flow-based approach for Trickbot banking trojan detection / A. Gezer [et al.] // Computers & Security. – 2019. – Vol. 84. – P. 179–192.

824. Szopinski, T. Factors affecting the adoption of online banking in Poland / T. Szopinski // Journal of Business Research. – 2016. – Vol. 69 (11). – P. 4763–4768. – DOI: 10.1016/j.jbusres.2016.04.027.

825. Lopez, P. Hardware trojans against virtual keyboards on e-banking platforms- a proof of concept / P. Lopez, H. Martin // AEU-International Journal of Electronic Communications. – 2017. – Vol. 76. – P. 146–151. – DOI: 10.1016/j.aeue.2017.04.003.

826. Киберугрозы для финансовых организаций в 2021 году: отчет Лаборатории Касперского GReAT. – 2020. – Режим доступа: https://securelist.ru/cyberthreats-to-financial-organizations-in-2021/99420/ (дата обращения: 15.03.2021).

827. Kessem, L. Its attack scope in Spain, brings redirection attacks to local banks / L. Kessem, T. Widens. – 2017. – URL: https://securityintelligence.com/TrickBot-habla-espanol-trojan-widens-its-attack-scope-in-spain-brings-redirection-attacks-to-local-banks (date of access: 07.12.2018).

828. A taxonomy of botnet behavior, detection, and defense / S. Khattak [et al.] // IEEE Communications Surveys & Tutorials. – 2014. – Vol. 16 (2). – P. 898–924.

829. Мошенники не щадят банковских клиентов // Коммерсантъ. – 2021. – Режим доступа: https://www.kommersant.ru/doc/4897743?tg (дата обращения: 10.08.2021).

830. Буйлов, М. Интернет вещей пришел за деньгами. Российские банки отразили крупнейшую DDoS-атаку / М. Буйлов, К. Дементьева, Ю. Степанова // Коммерсантъ. – 2021. – С. 7. – Режим доступа: https://www.kommersant.ru/doc/4968082 (дата обращения: 21.10.2021).

831. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств / Банк России. – 2021. – Режим доступа: https://www.cbr.ru/analytics/ib/review_2q_2021/ (дата обращения: 08.10.2021).

832. Cyber attack models for smart grid environments / P. Eder-Neuhauser [et al.] // Sustainable Energy, Grids and Networks. – 2017. – Vol. 12. – P. 10–29. – DOI: 10.1016/j.segan.2017.08.002.

833. Bhardwaj, A. Cyber security attacks on robotic platforms / A. Bhardwaj, V. Avasthi, S. Goundar // Network Security. – October 2019. – P. 13–19.

834. Papakostas, N. A novel paradigm for managing the product development process utilising blockchain technology principles / N. Papakostas, A. Newell, V. Hargaden // CIRP Annals – Manufacturing Technology. – 2019. – Vol. 68. – P. 137–140.

835. Simon, J. Cybersecurity investments in the supply chain: Coordination and a strategic attacker / J. Simon, A. Omar // European Journal of Operational Research. – 2019. – 11 p. – DOI: 10.1016/j.ejor.2019.09.017 0377-2217.

836. Ferrag, M. Security Solutions and Applied Cryptography in Smart Grid Communications / M. Ferrag, A. Ahmim. – Hershey: IGI Global, 2016. – 464 p. – DOI: 10.4018/978-1-5225-1829-7.

837. Securing Smart Grid: Cyber Attacks, Countermeasures, and Challenges / X. Li [et al.] // IEEE Communications Magazine. – 2012. – Vol. 50, no. 8. – P. 38–45. – DOI: 10.1109/MCOM.2012.6257525.

838. Kitchin R. Getting Smarter About Smart Cities: Improving Data Privacy and Data Security: Department of the Taoiseach, Data Protection Unit / R. Kitchin. – Dublin, Ireland, 2016. – URL: http://www.taoiseach.gov.ie/eng/Publications/Publications_2016/Smart_Cities_Report_January_2016.pdf (date of access: 07.06.2019).

839. Bailey, T. The energy-sector threat: How to address cybersecurity vulnerabilities: McKinsey Report / T. Bailey, A. Maruyama, D. Wallance. – November 2020. – 12 p. – URL: https://www.mckinsey.com/~/media/mckinsey/business%20functions/risk/our%20insights/the%20energy%20sector%20threat%20how%20to%20address%20cybersecurity%20vulnerabilities/the-energy-sector-threat-how-to-address-cybersecurity-vulnerabilities-f.pdf?shouldIndex=false (date of access: 16.02.2021).

840. Cyber-physical Vulnerabilities in Additive Manufacturing Systems: A Case Study Attack on the. STL file with human subjects / L. Sturm [et al.] // Journal of Manufacturing Systems. – 2017. – Vol. 44. – P. 154–164.

841. Stark, M. Innovations in Digital Modelling for Next Generation Manufacturing System Design / M. Stark, S. Kind, S. Neumeyer // Manufacturing Technology. – 2017. – Vol. 66 (1). – P. 169–172.

842. Lee, R. Analysis of the Cyber Attack on the Ukrainian Power Grid: Electricity Information Sharing and Analysis Center (E-ISAC) / R. Lee, M. Assante, T. Conway. – 2016. – 30 p. – URL: https://nsarchive.

gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdf (date of access: 17.06.2019).

843. Sharma, S. A survey on internet of vehicles: Applications, security issues & solutions / S. Sharma, B. Kaushik // Vehicular Communications. – 2019. – P. 1–44.

844. Manvi, S. A survey on authentication schemes in VANETs for secured communication / S. Manvi, S. Tangade // Vehicular Communications. – 2017. – Vol. 9. – P. 19–30.

845. Mahdavifar, S. Application of deep learning to cybersecurity: A survey / S. Mahdavifar, A. Ghorbani // Neurocomputing. – 2019. – Vol. 347. – P. 149–176. – DOI: 10.1016/j.neucom.2019.02.056.

846. Malecki, F. StorageCraft. Best practices for preventing and recovering from a ransomware attack / F. Malecki // Computer Fraud & Security. – 2019. – P. 8–10.

847. Annual number of ransomware attacks worldwide from 2014 to 2020 / Statista. – 2020. – URL: https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/ (date of access: 14.06.2020).

848. Ransomware is Costing UK Companies £346 Million Per Annum to their Bottom Line. – 2017. – URL: https://www.sentinelone.com/press/ransomware-costing-uk-companies-346-million-per-annum/ (date of access: 18.11.2020).

849. Ransomware 2021. Critical Mid-Year Update: Chainalysis. – 2021. – 38 p. – URL: https://go.chainalysis.com/rs/503-FAP-074/images/Ransomware-2021-update.pdf (date of access: 03.06.2020).

850. Luh, R. AIDIS: Detecting and classifying anomalous behavior in ubiquitous kernel processes / R. Luh, H. Janicke, S. Schrittwieser // Computers & Security. – 2019. – Vol. 84 (C). – P. 120–147. – DOI: 10.1016/j.cose.2019.03.015.

851. Sood, A. Targeted cyberattacks: a superset of advanced persistent threats / A. Sood, R. Enbody // IEEE Security & Privacy. – 2013. – Vol. 1. – P. 54–61.

852. Chien, E. W32. Duqu: the precursor to the next Stuxnet / E. Chien, L. O'Murchu, N. Falliere // Proceedings of the fifth USENIX workshop on large-scale exploits and emergent threats (LEET). – 2012. – URL: https://www.usenix.org/conference/leet12/workshop-program/presentation/chien (date of access: 25.08.2021).

853. The DUQU 2.0 Technical Details Version: 2.1. – 2015. – 46 p. – URL: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07205202/The_Mystery_of_Duqu_2_0_a_sophisticated_cyberespionage_actor_returns.pdf (date of access: 24.01.2020).

854. Maestre V. Swarm and Evolutionary Computation / V. Maestre. – 2017. – 15 p. – DOI: 10.1016Zj.swevo.2017.07.002.

855. Europol. The Internet Organized Crime Threat Assessment (iOCTA). – 2015. – URL: http://www. europol.europa.eu (date of access: 11.10.2019).

856. Kurtz, J. Noncivilian Government Context / J. Kurtz // Hacking Wireless Access Points Cracking, Tracking, and Signal Jacking. – 2017. – P. 109–128. – DOI: 10.1016/B978-0-12-805315-7.00008-5.

857. Robinson, N. Distributed denial of government: the Estonian Data Embassy Initiative / N. Robinson, K. Martin // Network Security. – 2017. – Vol. 9. – P. 13–16. – DOI: 10.1016/S1353-4858(17)30114-9.

858. Cyber-security Strategy 2009–2013: Ministry of Economic Affairs & Communications. – Estonia, 2008. – URL: https://www. cyberwiser.eu/estonia-ee (date of access: 11.07.2020).

859. Winkler, I. Adversary Infrastructure / I. Winkler, A. Gomes // Advanced Persistent Security. – 2017. – Chapter 7. – P. 67–79. – DOI:10.1016/B978-0-12-809316-0.00007-5.

860. Risk, resilience, and rebalancing in global value chains / McKinsey Global Institute. – 2020. – 112 p. – URL: https://www. mckinsey.com/~/media/McKinsey/Business%20Functions/Operations/Our%20Insights/ Risk%20resilience%20and%20rebalancing%20in%20global%20value%20chains/Risk-resilience-and-rebalancing-in-global-value-chains-full-report-vH.pdf (date of access: 15.11.2020).

861. Zhang, T. A comparative study on sanction system of cyber aider from perspectives of German and Chinese criminal law / T. Zhang // Computer Law & Security Review: The International Journal of Technology Law and Practice. – 2017. – Vol. 33 (1). – P. 98–102. – DOI: 10.1016/j.clsr.2016.11.017.

862. Ransomware threat success factors, taxonomy, and countermeasures: a survey and research direction / B. Al-Rimy [et al.] // Computers & Security. – 2018. – Vol. 74. – P. 144–166. – DOI: 10.1016/j.cose.2018.01.001.

863. Goncharov, M. Russian Underground 101: Trend Micro Incorporated. Research Paper / M. Goncharov. – 2012. – 29 p. – URL: https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf?_ga=2.259319754.1186463633.1634981178-1453004565.1634981175 (date of access: 03.11.2019).

864. PandaLabs Q1 Report: Trojans Account for 80% of Malware Infections / Set New Record. Panda Security. – 2013. – URL: http://

www.pandasecurity.com/mediacenter/press-releases/pandalabs-q1-report-trojans-account-for-80-of-malware-infections-set-new-record/ (date of access: 06.02.2020).

865. Glenny, M. Darkmarket: Cyberthieves, Cybercops and You / M. Glenny. – Canada: Random House, 2011. – 107 p.

866. Davies, C. Welcome to DarkMarket – Global One-stop Shop for Cybercrime and Banking Fraud / C. Davies // The Guardian. – 2010. – URL: https://www.theguardian.com/technology/2010/jan/14/darkmarket-online-fraud-trial-wembley (date of access: 03.08.2019).

867. Leyden, J. DarkMarket Carder Forum Revealed as FBI Sting / J. Leyden. – URL: http://www.theregister.co.uk/2008/10/14/darkmarket_sting/ (date of access: 03.08.2019).

868. Chabinsky S. The Cyber Threat: Who's Doing What to Whom? S. Chabinsky // US Federal Bureau of Investigation. – URL: https://www.fbi.gov/news/speeches/the-cyber-threat-whos-doing-what-to-whom (date of access: 25.09.2018).

869. Степанова, Ю. Криминал перешел в Интернет / Ю. Степанова // Коммерсантъ. – 2020. – Режим доступа: https://www.kommersant.ru/doc/4544119?tg (дата обращения: 23.10.2020).

870. Cyber Security Insights: Report Global Results / Norton. – 2018. – 44 p. – URL: file:///C:/Users/~/AppData/Local/Temp/MicrosoftEdgeDownloads/5d5e75be-bf7c-49df-9544-49b08316bc28/2018-norton-lifelock-cyber-safety-insights-report-global-results-en.pdf (date of access: 18.02.2019).

871. Cybercrime victimization and subjective well-being: An examination of the buffering effect hypothesis among adolescents and young adults / M. Kaakinen [et al.] // Cyberpsychology, Behavior, and Social Networking. – 2018. – Vol. 21. – P. 129–137.

872. Srimoolanathan, A. Protecting privacy: are today's national laws a boon or bane? / A. Srimoolanathan // Biometric Technology Today. – 2019. – Vol. 10. – P. 8–11. – DOI: 10.1016/S0969-4765(19)30143-2.

873. Identity Threat and Assessment Prediction (ITAP): University of Texas at Austin Center for Identity. – 2019. – URL: https://identity.utexas.edu/research-projects/identity-threat-and-assessment-prediction-itap (date of access: 23.02.2020).

874. Future Series: Cybersecurity, emerging technology and systemic risk / Insight Report World Economic Forum. – 2020. – 59 p. – URL: http://www3.weforum.org/docs/WEF_Future_Series_Cybersecurity_emerging_technology_and_systemic_risk_2020.pdf (date of access: 04.15.2021).

875. Cyber Security: Export Strategy / Department for International Trade. – 2018. – 20 p. – URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/693989/CCS151_CCS0118810124-1_Cyber_Security_Export_Strategy_Brochure_Web_Accessible.pdf (date of access: 26.03.2020).

876. Morgan, S. Global Cybersecurity Spending Predicted To Exceed $1 Trillion From 2017-2021 / S. Morgan // Cybercrime Magazine. – 2019. – URL: https://cybersecurityventures.com/cybersecurity-market-report/ (date of access: 15.12.2020).

877. Threat Forecasting. Leveraging Big Data for Predictive Analysis / J. Pirc [et al.]. – Cambridge: Elsevier. 2016. – P. 1–15. – DOI: 10.1016/B978-0-12-800006-9.00001-X.

878. Global Cybersecurity Outlook 2022: Insight Report. – 2022. – 35 p. – URL: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf (date of access: 20.01.2022).

879. Bischoff, P. How data breaches affect stock market share prices: Comparitech / P. Bischoff. – 2021. – URL: https://www.comparitech.com/blog/information-security/data-breach-share-price-analysis/#NASDAQ_benchmark_validation (date of access: 24.12.2021).

Научное издание

Криштаносов Виталий Брониславович

ЦИФРОВИЗАЦИЯ ЭКОНОМИКИ РЕСПУБЛИКИ БЕЛАРУСЬ И НАЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ: СОВРЕМЕННЫЕ КОНЦЕПТУАЛЬНО-АНАЛИТИЧЕСКИЕ ПОДХОДЫ

Монография

В 2-х томах

Том 1

Редактор *Р. М. Рябая*
Компьютерная верстка *В. А. Маркушевская*
Дизайн обложки *П. П. Падалец*
Корректор *Р. М. Рябая*

Подписано в печать 25.01.2023. Формат $60\times84^{1}/_{16}$.
Бумага офсетная. Гарнитура Таймс. Печать ризографическая.
Усл. печ. л. 20,2. Уч.-изд. л. 22,0.
Тираж 100 экз. Заказ .

Издатель и полиграфическое исполнение:
УО «Белорусский государственный технологический университет».
Свидетельство о государственной регистрации издателя,
изготовителя, распространителя печатных изданий
№ 1/227 от 20.03.2014.
Ул. Свердлова, 13а, 220006, г. Минск.