**РОССИЙСКАЯ АКАДЕМИЯ НАУК**

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**Федеральное государственное бюджетное учреждение науки**
**Институт научной информации по общественным наукам**
**Российской академии наук**
**(ИНИОН РАН)**

# СОЦИАЛЬНЫЕ НОВАЦИИ И СОЦИАЛЬНЫЕ НАУКИ

**Научный журнал**

**№ 1 (1) / 2020**

## ЦИФРОВИЗАЦИЯ И БЕЗОПАСНОСТЬ: ЛИЧНОСТЬ, БИЗНЕС, ГОСУДАРСТВО

**Издается с 2020 г.**

**Выходит 4 раза в год**

Составитель номера –

канд. юр. наук С.И. Коданева

**Москва 2020**

Учредитель:
Федеральное государственное бюджетное учреждение науки
Институт научной информации по общественным наукам
Российской академии наук (ИНИОН РАН)

## *Редакция*



DOI: 10.31249/snsn/2020.01.00

## *СОДЕРЖАНИЕ*

## Дорогие читатели!

Перед вами первый номер журнала «Социальные новации и социальные науки». Издание направлено на развитие диалога между представителями различных наук об обществе и создание «обратной связи» между авторами и читателями. Представляется, что даже на фоне огромного потока научной периодики сохраняется востребованность площадок, которые способствуют преодолению междисциплинарных барьеров при изучении сложных социальных явлений, переходу от анализа к синтезу нового знания и выработке конструктивных практических рекомендаций.

Когда задумывался этот номер – в благополучном, как теперь кажется, 2019 году, – никто не мог предвидеть, насколько актуальной станет его тема – *тема безопасности,* – и какие новые аспекты она получит.

Конечно, вопросы безопасности относятся к «вечным». Развиваясь, общество преодолевает какие-то проблемы в этой области, однако возникают новые. Одним из таких неоднозначных феноменов является процесс цифровизации. В условиях пандемии он резко ускорился, изменяя образ жизни миллионов людей. Одновременно все более очевидными становятся его позитивные и негативные социальные последствия.

Современная реальность представляет собой сложный клубок старых и новых проблем. Поиски их решений требуют объединения усилий специалистов самых разных дисциплин и научных направлений. Перед научным сообществом встают новые задачи – и мы должны найти ответы на новые вызовы!

Главный редактор канд. геогр. наук
*М.А. Положихина*

# ПРЕДСТАВЛЯЕМ НОМЕР

Тема первого выпуска журнала «Социальные новации и социальные науки» выбрана не случайно. Развитие цифровых технологий в условиях информационной революции и глобализации экономики приводит к возникновению системообразующих новаций не только в технологической, но, возможно, даже в большей степени в социальной сфере. В настоящий момент многие из них позволяют справляться с бедами пандемии – удаленная работа, дистанционное обучение и общение, электронный банкинг. Мир постепенно, но кардинально трансформируется: меняются способы взаимодействия между людьми, между обществом и государством, а также способы ведения бизнеса, но главное – меняется система ценностей.

Происходящие процессы принято называть четвертой промышленной революцией, а для формирующейся новой системы предлагаются разные названия – «цифровая экономика», «сетевая экономика», «экономика знаний» и т.д. Причем скорости изменений в разных подсистемах не совпадают. Обычно преобразования в технической сфере происходят значительно быстрее, чем в социально-экономической сфере и общественном сознании. Однако в последнее время темпы их трансформации заметно ускорились.

Что несут нам эти социальные новации? Как всегда бывает во времена радикальных перемен, общество и ученые разделились на два лагеря. С одной стороны, «революционеры», которые приветствуют быстрое развитие новых технологий, связывая с ними перспективы экономического роста и решения многих социальных проблем. С другой стороны, «консерваторы», которые относятся к новым технологиям с опасением, видя в них множество рисков и угроз.

Опасения по поводу ускорения процесса цифровизации усиливаются из-за того, что система государственно-правового регулирования явно отстает от вызовов новых технологических возможностей. Много нерешенных вопросов сохраняется в области обеспечения кибербезопасности, регулирования электронной торговли и Интернета, правил использования биоинженерных технологий, беспилотных транспортных средств, 3D-принтеров, искусственного интеллекта и т.д. Общественное сознание будоражат фильмы о вышедших из-под контроля роботах, киборгах, человеко-компьютерных монстрах и т.п. Рекламодатели соблазняют «умными» домами, «говорящими» утюгами и холодильниками. Продвинутые архитекторы предлагают правительствам строить «умные» города. В то же время информатизация систем управления остается наиболее коррупциоген-

ной сферой, поглощающей все большую часть бюджетов органов управления без сколько-нибудь заметной отдачи. Обостряются такие негативные проявления цифровизации, как кибермошенничество, распространение фейковых новостей и т.д.

Однако, несмотря на все эти опасения, невозможно не признавать важность новых технологий для развития общества и государства. Именно технические инновации были и остаются одним из основных драйверов общественного прогресса.

В то же время нельзя не видеть и риски, всегда появляющиеся вместе с новым знанием. Осознание этих рисков должно давать толчок к их преодолению. Главное – понимать, что со временем новые технологии изменят все то, что сегодня воспринимается как должное, – от механизмов производства товаров и услуг до инструментов и форм трудовой деятельности, общения и восприятия окружающего мира. Но то, как изменится мир, зависит все-таки от нас самих.

Важно также отметить, что развитие технологий – это постоянный и непрерывный процесс. Новые технологии будут продолжать появляться и вновь изменять наш мир. В то же время человечество не перестает сталкиваться с вызовами и угрозами естественного, природного характера. Такие ситуации становятся своего рода «контрольными точками», когда общество получает возможность проверить, насколько накопленные новации позитивны и устойчивы.

Ярким примером подобного испытания стала пандемия COVID-19. Она протестировала способность человечества противостоять глобальным угрозам, риск которых многократно усиливается в случае неконтролируемого развития биотехнологий и биоинженерии с использованием современных цифровых технологий. Также была продемонстрирована важность обеспечения биозащищенности и биобезопасности всех граждан. Вместе с тем наглядно проявились преимущества и возможности различных цифровых технологий, которые стали незаменимыми помощниками в условиях борьбы с коронавирусом.

Актуальные вопросы современности рассматриваются в материалах авторов журнала. В обычае издания вести обсуждение непредвзято и всесторонне, в различных ракурсах и контекстах. Слово предоставляется как авторитетным, так и молодым специалистам, освещающим проблемы с разных позиций и уровней.

Открывает номер рубрика ***«Пространство дискурса: цифровизация и безопасность»***, в которой представлены статьи, предлагающие читателям разные взгляды на проблемы обеспечения безопасности человека, общества и государства в условиях цифровизации. В статье *М.А. Положихиной* анализируются угрозы безопасности, обусловленные распространением новых информационно-коммуникационных технологий, подчеркивается системное воздействие последних на общественное развитие. *С.А. Стрижов* исследует влияние цифровизации на устойчивое развитие России, с акцентом на кризисные ситуации, подобные пандемии COVID-19. *В.К. Лева-*

*шов и В.К. Сарьян* обращаются к вопросам устойчивого функционирования национальных информационных систем и систем управления. Завершает раздел работа *А.А. Зацаринного*, который рассматривает проблемы организации научной деятельности в условиях цифровизации.

В разделе ***«Точка зрения»*** представлены работы, раскрывающие специфику цифровой безопасности в отдельных отраслях. Открывает раздел статья *В.В. Коровкина*, в которой анализируются перспективы и проблемы формирования международного правового регулирования киберпространства. Последнее признается общественным благом, принадлежащим всему человечеству, но подверженным различным угрозам. Наиболее значимо из них хакерство, подрывающее безопасность критически важных объектов и целых сфер деятельности. Проблематика современной безопасности финансового сектора отражена в статье *Г.В. Семеко.* Материал *В.П. Куприяновского, А.А. Климова и О.Н. Покусаева* раскрывает важность формирования единых правил (онтологий) в сфере электронных закупок. Две последующие статьи связаны с проблемами защиты здоровья людей. *Н.А. Коровникова* рассматривает состояние и риски ментальной безопасности в цифровую эпоху, а также раскрывает взаимосвязь ментальной, образовательной и национальной безопасности в контексте цифровизации. В статье *А.А. Карцхии* представлен подробный анализ правового регулирования биобезопасности на международном уровне, в законодательстве зарубежных стран и России.

В материалах рубрики ***«Человек в цифровом мире»*** поднимаются вопросы, важные для каждого человека. Так, *А.А. Петров* раскрывает возможности сбора сведений о человеке из различных источников (включая Интернет и социальные сети) и способы их анализа, а также направления последующего использования полученных данных. Продолжает тему защищенности персональных данных *А.П. Иванова*, которая анализирует современные механизмы страхования утечки данных. Завершает раздел статья *С.И. Коданевой*, посвященная проблеме психологической зависимости молодежи от социальных сетей. В ней отмечается, что в последнее время все большее распространение получает такое явление как кибербуллинг – умышленное причинение психического вреда жертве, не способной себя защитить. Обеспечение кибербезопасности подрастающего поколения и общества в целом требует специальных мер противодействия.

***«Профессиональный взгляд»*** – заключительная рубрика журнала, в которую вошла рецензия *А.В. Костиной* на монографию Т.Ф. Кузнецовой «Цифровое общество, цифровая культура и гуманитаризация высшего образования: тезаурусный подход». Автор книги рассматривает период зарождения цифровой культуры в России – момент формирования новых тенденций культурной жизни. Представляется крайне важным их вовремя заметить и осмыслить, опираясь на многовековые традиции мировой и отечественной культуры.

Надеемся, что публикация материалов номера будет способствовать конструктивному обсуждению в рамках социальных наук актуальных проблем цифровой трансформации современного общества.

Составитель номера канд. юр. наук

*С.И. Коданева*

# ПРОСТРАНСТВО ДИСКУРСА: ЦИФРОВИЗАЦИЯ И БЕЗОПАСНОСТЬ

## ВЛИЯНИЕ ЦИФРОВИЗАЦИИ НА БЕЗОПАСНОСТЬ: ОТ ИНДИВИДУУМА ДО СОЦИУМА

**Положихина Мария Анатольевна**

Кандидат географических наук, ведущий научный сотрудник Отдела экономики Института научной информации по общественным наукам РАН (ИНИОН РАН), (Москва, Россия)

***Аннотация.*** *Анализируются угрозы безопасности, обусловленные распространением новых информационно-коммуникационных технологий и процессом цифровизации. Подчеркивается системное влияние новых технологий на общественное развитие и важность определения последствий для создания общей теории безопасности.*

***Ключевые слова:*** *безопасность; цифровизация; риски цифровизации; обеспечение цифровой безопасности.*

**Для цитирования:** Положихина М.А. Влияние цифровизации на безопасность: от индивидуума до социума // Социальные новации и социальные науки. – Москва: ИНИОН РАН, 2020. – № 1. – С. 9–27.

URL: https://sns-journal.ru/ DOI: 10.31249/snsn/2020.01.01

## Введение

Тема безопасности достаточно традиционна для социальных наук, поскольку связана с фундаментальными представлениями о человеке и обществе. Однако с течением времени взгляды на безопасность существенно менялись. Продолжают развиваться они и в настоящее время.

С Античности до Нового времени безопасность рассматривалась преимущественно с точки зрения ограждения от насилия личности, системы власти и государства. Более того, обеспечение безопасности было и продолжает оставаться одной из главных государственных функций, а также основной деятельностью ряда важнейших институтов (армии, разведки и контрразведки, полиции, судебной системы). Сведение безопасности к противостоянию внешнему и внутреннему насилию определяло преобладание подходов к ней с военной и правовой позиций, что обусловило распространение данной проблематики в теории государства и права и международных отношений.

По мере развития общества потребности в безопасности стали разнообразнее и масштабнее. Мировые войны, техногенные и экологические катастрофы, революции и социально-экономические кризисы XX в. привели к прорыву в представлениях о безопасности и преодолению традиционного взгляда на нее как преимущественно военную (силовую). Признание глобального характера безопасности, выделение разных ее видов и акцент на правах человека послужили причиной создания ряда международных организаций по обеспечению безопасности, а также экспансии концепции безопасности во все общественные дисциплины. В науке и практике все больше внимания стало уделяться невоенным аспектам безопасности.

К началу XXI в. преобразование человеком среды обитания с помощью разнообразной техники и технологий позволило добиться значительного роста комфорта и безопасности, усиления влияния на природные процессы и объекты. Однако одновременно стало увеличиваться количество и масштабы угроз для самой человеческой жизнедеятельности. Возросли турбулентность социально-экономических и природных процессов, степень неопределенности общественного развития. Усиливающаяся зависимость природных и социально-экономических систем от используемых технологий приводит к повышению их уязвимости и возникновению новых, не существовавших ранее рисков, что, в свою очередь, обусловливает возрастание значения вопросов безопасности.

Осознание современных масштабов угроз человечеству и биосистеме планеты в целом поставило вопрос о необходимости построения общей теории безопасности, которая позволила бы выявить весь комплекс проблем и прогнозировать опасные направления развития событий. Безусловно, такая теория должна основываться на междисциплинарном подходе и обобщении основных

положений частных концепций безопасности. И хотя шаги по выработке общей теории безопасности предпринимаются, для этого требуются усилия специалистов разных научных направлений.

Цель данной статьи состоит в анализе угроз безопасности, которые определяются распространением новых информационно-коммуникационных технологий (ИКТ) и процессом цифровизации. В связи с системным влиянием новых технологий на общественное развитие такое исследование представляется важным для создания общей теории безопасности.

## Представления о безопасности и ее видах

Эволюция представлений о безопасности достаточно хорошо известна, и в целом она соответствует развитию теоретических взглядов на общество, государство и личность. Хотелось бы подчеркнуть, что длительное время безопасность трактовалась как защищенность (самосохранение и выживание) государства и его граждан от разного рода опасностей. Формирование современных научных концепций и непосредственные события XX в. привели к трансформации подходов к безопасности, соотнесению их с социально-экономическим благополучием и правами человека, а также экологической проблематикой.

В России вследствие особенностей исторического развития безопасность всегда в первую очередь рассматривалась с точки зрения безопасности государства, прежде всего в военной области, и носила прикладной технический характер. Можно говорить о национальной иерархии приоритетов безопасности: государственная обороноспособность, внутренняя стабильность, защита прав личности. Данный подход в модифицированном виде сохраняется и в настоящее время. Главные изменения связаны со значительным расширением представлений о безопасности.

В 1992 г. был принят первый российский закон о безопасности, в котором дано определение этого термина [Закон РФ «О безопасности» от 05.03.1992 № 2446–1, 1992]. С 1991 г. в российских школах появился курс «Основы безопасности жизнедеятельности», в 1993 г. – утверждена учебная специальность «Безопасность жизнедеятельности» для вузов. В начале 1990-х годов появились первые отечественные учебники по безопасности жизнедеятельности для школ и вузов, в которых излагались существующие на тот момент знания по безопасности. Обновился корпус законодательных актов, касающихся разных аспектов безопасности, который был создан в советское время. В 2000-е годы количество научной и образовательной литературы, а также официальных документов по вопросам безопасности в России значительно увеличилось.

Анализ баз данных ИНИОН РАН за период с 1991 по 2018 г. позволяет проследить изменения в публикационной активности отечественных специалистов из разных общественных дисциплин по проблемам безопасности (табл. 1).

Как следует из приведенных данных, научный интерес к теме за рассматриваемый период значительно вырос: общее количество публикаций, так или иначе касающихся вопросов безопас-

ности, увеличилось в 9,3 раза. Причем если количество публикаций по проблемам безопасности политологического и правоведческого характера (база данных по государству и праву) возросло за 27 лет в 7 раз, то экономико-демографического направления – в 11,5 раза, а в философии и социологии – в 24,6 раза. Соответственно изменилась структура информационного потока, что отражает определенное смещение приоритетов.

Таблица 1

**Встречаемость понятия «безопасность» в названиях публикаций на русском языке в базах данных ИНИОН РАН за соответствующий год, ед. ***

| № пп | Годы | База данных по экономике и демографии | База данных по государству и праву | База данных по философии и социологии | В целом |
|---|---|---|---|---|---|
| 1. | 1991 | 20 | 52 | 5 | 77 |
| 2. | 1998 | 90 | 240 | 26 | 356 |
| 3. | 2005 | 92 | 338 | 52 | 482 |
| 4. | 2012 | 98 | 269 | 99 | 466 |
| 5. | 2018 | 230 | 365 | 123 | 718 |

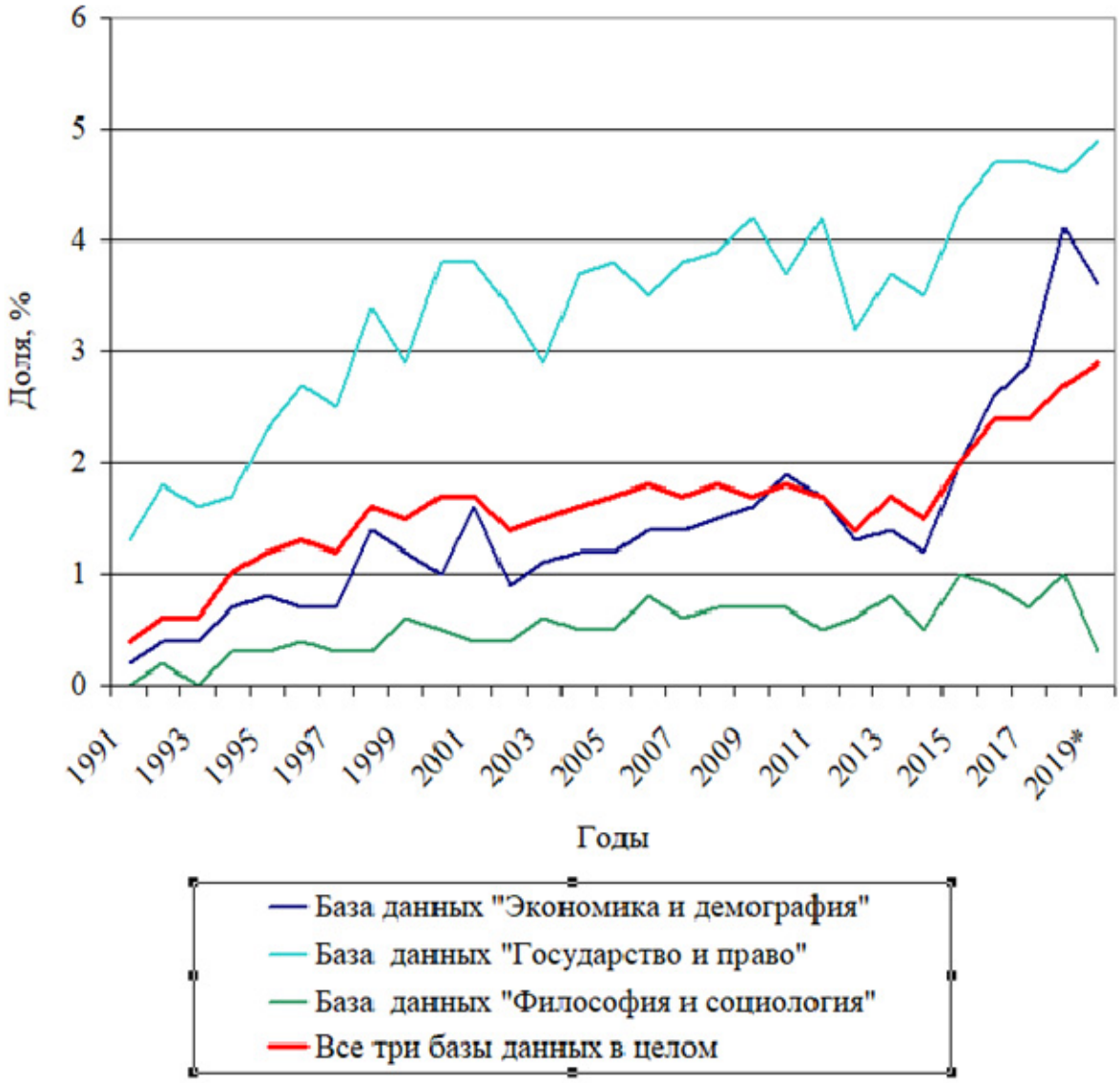
* Источник: составлено автором.

В 1991 г. большая часть публикаций, связанных с вопросами безопасности, традиционно приходилась на теорию государства и права и политологию – более 67% от общего количества публикаций на данную тему. В других общественных дисциплинах интерес к вопросам безопасности был значительно ниже: на публикации экономического и демографического характера приходилось 26%, социологического и философского характера – около 7% от общего количества публикаций на данную тему. К 2018 г. доля работ политологического и правоведческого характера снизилась до 51% от общего количества публикаций на данную тему. Почти сравнялись с ними масштабы публикаций по вопросам безопасности экономического и демографического характера – 32% от их общего количества. Возросла до 17% соответственно доля публикаций по вопросам безопасности социологического и философского характера.

Однако в целом интерес в общественных науках к проблемам безопасности не очень широк. Согласно базам данных ИНИОН РАН, в 1991 г. доля публикаций по этим вопросам в общем количестве работ общественно-научного направления составляла 0,4% (с колебаниями от почти 0% в философии и социологии, 0,2 – в экономике и демографии до 1,3% в политологии и правоведении). В 2018 г. доля публикаций, касающихся вопросов безопасности, в общем количестве работ общественно-научного направления увеличилась до 2,7% (0,3% в философии и социологии, 3,6 – в экономике и демографии, 4,9% в политологии и правоведении).

Интенсивность внимания к проблемам безопасности различается не только по отдельным общественным дисциплинам, но и по разным временным периодам. Изменение относительной частоты встречаемости (доли) термина «безопасность» в названиях русскоязычных публикаций (измеряемой в процентах от их общего количества), включенных в базы данных ИНИОН РАН, в

1991–2019 гг. позволяет выявить не только весьма неравномерную динамику, но и некоторые ее закономерности (рис. 1).




* 2019 г. – предварительные данные.

**Рис. 1. Изменение доли термина «безопасность» в названиях русскоязычных публикаций, включенных в базы данных ИНИОН РАН, за период 1991–2019 гг.**

Общая тенденция роста научного интереса к вопросам безопасности выражается в увеличении количества соответствующих публикаций в общем информационном потоке, а следовательно, и относительной частоты встречаемости термина «безопасность» в их названиях.

Наиболее ярко такая поступательная динамика прослеживается в базах данных «Экономика и демография» и «Государство и право», а база данных «Философия и социология» демонстрирует скорее ее колебательный характер. На этом фоне можно выделить три «волны» усиления внимания отечественных специалистов к вопросам безопасности: с 1991 по 2001 г., с 2003 по 2010 г. и с 2015 г. по настоящее время.

При этом в разных базах данных границы периодов роста и снижения интереса к теме безопасности могут несколько смещаться по отношению к общей картине. Тем не менее выявляются «пики» научного интереса к данной теме, которые приходятся на 2000, 2010 и 2018 гг. Наоборот, в 2002 г. и в 2011–2014 гг. в отечественной научной литературе наблюдалось снижение интереса к вопросам безопасности (рис. 1.).

Выявленная динамика (при учете существования временного лага между написанием и публикацией научных работ) позволяет констатировать, что в них преобладает рефлексия на уже свершившиеся события.

Более того, максимальное снижение внимания к проблемам безопасности в предкризисные периоды свидетельствует о крайне низкой степени прогностичности имеющихся научных знаний по данному направлению. Безусловно, повышение уровня неопределенности современного общественного развития во многом определяет неожиданность возникновения опасных событий (кризисов). Но не меньшее значение имеет недостаточная проработанность общей теории безопасности, недоучет связей между различными аспектами безопасности, игнорирование критериев и параметров безопасного развития, а также слабо развитый и непоследовательный их мониторинг.

Хотя следует признать, что нормативная и научно-образовательная деятельность конца XX – начала XXI в. позволила достичь определенного прогресса в представлениях о безопасности.

В самом общем смысле «безопасность» означает «положение, при котором не угрожает опасность кому-нибудь или чему-нибудь», или состояние защищенности от опасности (ей). Современное употребление этого термина тесно связано с такими понятиями, как «риск», «угроза», «вызов». В общем контексте они означают:

– риск – вероятность какого-либо опасного (неблагоприятного) события (явления, процесса) или его развития (последствия);

– угрозы – опасные (неблагоприятные) условия или факторы (явления, процессы), действие (воздействие) которых могут привести к какому-либо ущербу (вреду);

– вызовы – факторы (явления, процессы), способные при определенных условиях привести к возникновению угроз, т.е. потенциально опасные.

При этом существуют самые разнообразные определения всех этих терминов. Основными в современных представлениях о безопасности можно считать следующие: 1) безопасность как состояние защищенности жизненно важных интересов личности, государства, общества от внутренних и внешних угроз; 2) безопасность как состояние системы, при котором действие внешних и внутренних факторов не приводит к невозможности ее функционирования.

Первое определение базируется на политико-правовом подходе к безопасности и соответствует трактовке Закона РФ «О безопасности» и основанных на нем документов [Закон РФ «О безопас-

ности» от 05.03.1992 № 2446–1, 1992]. Второе отвечает технико-управленческому подходу к данному феномену. Притом что один подход не противоречит другому, специалисты из соответствующих дисциплин, обсуждая вопросы безопасности, как бы говорят на разных языках и нуждаются в определенном «переводчике». Необходимо отметить, что для всех общественных (социальных) наук естественен первый подход. Данная статья также основывается на этом подходе к безопасности. Но создание общей теории безопасности требует максимального сближения (конвертации) подходов.

Выделяются различные частные виды безопасности.

В 1994 г. ПРООН (Программа развития ООН) определила семь основных категорий (видов) безопасности человека, в том числе: экономическую, продовольственную, безопасность для здоровья, экологическую, личную (от физических пыток, войн, этнических конфликтов, преступных группировок, от насилия, жестокого обращения в семье с женщинами и детьми, от самоубийств и наркотиков), общественную и политическую [New Dimensions of Human Security, 1994, p. 24]. В Федеральном законе «О безопасности» 2010 г. перечислено четыре основных вида национальной безопасности: безопасность государства, общественная безопасность, экологическая безопасность, безопасность личности, но список не является исчерпывающим [Федеральный закон от 28.12.2010 № 390-ФЗ, 2010]. В словаре основных понятий и определений «Геополитика и национальная безопасность» 1998 г. было выделено 46 видов безопасности [Геополитика и национальная безопасность, 1998]. Современные литературные источники позволяют идентифицировать более 90 видов безопасности (табл. 2), причем этот перечень не является окончательным.

Резкий рост частных видов безопасности обусловил неоднократные попытки их систематизации и классификации. Наиболее распространенные способы представлены в табл. 2.

Таблица 2

**Классификация видов безопасности***

| № пп | Принципы классификации | Виды безопасности |
|---|---|---|
| 1 | 2 | 3 |
| 1. | По объектам | личности; детства; молодежи;<br>предприятия; бизнеса;<br>общества / социума; уголовно-исправительной системы;<br>государства;<br>природной / окружающей среды; экосистемы;<br>природного объекта;<br>международная; цивилизации; человечества и т.д. |
| 2. | По направлению воздействия | внешняя;<br>внутренняя;<br>гибридная |
| 3. | По уровням | глобальная; коллективная;<br>региональная (в том числе европейская; евразийская; центральноазиатская и т.д.);<br>национальная;<br>региона; территории;<br>поселения; города;<br>предприятия;<br>Индивидуальная |

| 1 | 2 | 3 |
|---|---|---|
| 4. | По сферам жизнедеятельности | военная (в том числе военно-политическая, пограничная);<br>политическая (в том числе этноконфессиональная);<br>экономическая (в том числе промышленная, продовольственная, энергетическая, инновационная, транспортная, внешнеторговая, военно-экономическая);<br>технологическая (в том числе эксплуатации разных видов транспорта, полетов, на море, дорожного движения, техника безопасности);<br>финансовая (в том числе налоговая, бюджетная, инвестиционная);<br>демографическая (в том числе миграционная);<br>социальная (в том числе кадровая, охрана труда, образования, медицинской помощи, потребительских товаров); экологическая;<br>информационная (в том числе связи и коммуникаций, кибербезопасность, компьютерная);<br>духовная (в том числе культуры, знания, лингвистическая, психологическая);<br>общественная;<br>пространственная (в том числе локальная) и т.д. |
| 5. | По видам угроз | природного характера (в том числе климатическая, сейсмическая, селевая, паводков и наводнений и т.д.);<br>антропогенного характера (в том числе отходов и т.д.);<br>пожарная;<br>чрезвычайных ситуаций;<br>от насилия;<br>наркобезопасность;<br>антитеррористическая;<br>ядерная;<br>радиационная;<br>химическая;<br>бактериологическая;<br>санитарно-эпидемиологическая;<br>комплексная (жизнедеятельности) и т.д. |

* Источник: составлена автором на основе баз данных ИНИОН РАН.

Очевидным недостатком большинства предложенных систем классификации является неограниченность видов безопасности. Так, при классификации по сферам жизнедеятельности можно смело повторять ОКВЭД (классификатор видов экономической деятельности) – ведь любой вид человеческой деятельности всегда сопровождается какими-либо рисками, нуждается в определенной технике безопасности и организации труда. При классификации по объектам или видам угроз тема безопасности превращается в безграничную область, так как кому-то или чему-то всегда может угрожать какая-то опасность. Относительную ограниченность видов безопасности обеспечивает их классификация по уровням, одновременно приводящая к признанию комплексного характера безопасности.

Логично, что следующим шагом стал переход от детализации к агрегированию видов безопасности. Соответственно, выделилось несколько крупных блоков безопасности: международная, национальная, общественная, личная, бизнеса, природной (окружающей) среды. Закономерно, что наибольшее внимание в России уделяется вопросам национальной безопасности. В принятых отечественных официальных документах стратегического характера даны определения национальной безопасности и отдельных ее видов, а также соответствующих им угроз, рисков и вызовов (табл. 3).

Таблица 3

## Определение отдельных видов безопасности*

| № пп | Источник | Определения |
|---|---|---|
| 1 | 2 | 3 |
| 1. | Стратегия национальной безопасности РФ [Указ Президента РФ от 31.12.2015 № 683] | Национальная безопасность – состояние защищенности личности, общества и государства от внутренних и внешних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан РФ, достойные качество и уровень их жизни, суверенитет, независимость, государственная и территориальная целостность, устойчивое социально-экономическое развитие РФ. Национальная безопасность включает в себя оборону страны и все виды безопасности, предусмотренные Конституцией РФ и законодательством РФ, прежде всего государственную, общественную, информационную, экологическую, экономическую, транспортную, энергетическую безопасность, безопасность личности;<br>Угроза национальной безопасности – совокупность условий и факторов, создающих прямую или косвенную возможность нанесения ущерба национальным интересам РФ |
| 2. | Стратегия экономической безопасности [Указ Президента РФ от 13.05.2017 № 208] | Экономическая безопасность – состояние защищенности национальной экономики от внешних и внутренних угроз, при котором обеспечиваются экономический суверенитет страны, единство ее экономического пространства, условия для реализации стратегических национальных приоритетов РФ;<br>Вызовы экономической безопасности – совокупность факторов, способных при определенных условиях привести к возникновению угрозы экономической безопасности;<br>Риск в области экономической безопасности – возможность нанесения ущерба национальным интересам РФ в экономической сфере в связи с реализацией угрозы экономической безопасности |
| 3. | Доктрина продовольственной безопасности [Указ Президента РФ от 21.01.2020 № 20] | Продовольственная безопасность – состояние социально-экономического развития страны, при котором обеспечивается продовольственная независимость РФ, гарантируется физическая и экономическая доступность для каждого гражданина страны пищевой продукции, соответствующей обязательным требованиям, в объемах не меньше рациональных норм потребления пищевой продукции, необходимой для активного и здорового образа жизни |
| 4. | Доктрина энергетической безопасности [Указ Президента РФ от 13.05.2019 № 216] | Энергетическая безопасность – состояние защищенности экономики и населения страны от угроз национальной безопасности в сфере энергетики, при котором обеспечивается выполнение предусмотренных законодательством РФ требований к топливо- и энергоснабжению потребителей, а также выполнение экспортных контрактов и международных обязательств РФ;<br>угроза энергетической безопасности – совокупность условий и факторов, создающих возможность нанесения ущерба энергетике РФ;<br>Вызов энергетической безопасности – совокупность условий и факторов, создающих новые стимулы для развития мировой энергетики или новые направления ее развития, но также способных привести к возникновению угрозы энергетической безопасности;<br>Риск в области энергетической безопасности – возможность перерастания вызова энергетической безопасности в угрозу реализации угрозы энергетической безопасности или наступления иных обстоятельств, оказывающих отрицательное влияние на состояние энергетической безопасности, в зависимости от действий или бездействия субъектов энергетической безопасности |
| 5. | Основы государственной политики РФ в области промышленной безопасности на период до 2025 г. и дальнейшую перспективу [Указ Президента РФ от 06.05.2018 № 198] | Промышленная безопасность – определяемое комплексом технических и организационных мер состояние защищенности промышленного объекта, которое характеризуется стабильностью параметров технологического процесса и исключением (сведением к минимуму) опасности возникновения аварии или инцидента, а в случае их возникновения – отсутствием опасности воздействия на людей опасных и вредных факторов и угрозы причинения вреда имуществу юридических и физических лиц, государственному или муниципальному имуществу |

| 1 | 2 | 3 |
|---|---|---|
| 6. | Концепция общественной безопасности (утв. Президентом РФ 20.11.2013) | Обеспечение общественной безопасности – реализация определяемой государством системы политических, организационных, социально-экономических, информационных, правовых и иных мер, направленных на противодействие преступным и иным противоправным посягательствам, а также на предупреждение, ликвидацию и (или) минимизацию последствий чрезвычайных ситуаций природного и техногенного характера;<br>Угроза общественной безопасности – прямая или косвенная возможность нанесения ущерба правам и свободам человека и гражданина, материальным и духовным ценностям общества |
| 7. | Доктрина информационной безопасности [Указ Президента РФ от 05.12.2016 № 646] | Информационная безопасность – состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие РФ, оборона и безопасность государства;<br>Угроза информационной безопасности – совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере |
| 8. | Федеральный закон от 10.01.2002 № 7-ФЗ «Об охране окружающей среды» | Экологическая безопасность – состояние защищенности природной среды и жизненно важных интересов человека от возможного негативного воздействия хозяйственной и иной деятельности, чрезвычайных ситуаций природного и техногенного характера, их последствий |

*Источник: составлена автором.

Обращает на себя внимание тот факт, что безопасность бизнеса не рассматривается в качестве составной части национальной безопасности. Более того, эта тема развивается во многом изолированно от обсуждения других вопросов безопасности. С одной стороны, у бизнеса немало собственных средств и организационных возможностей для обеспечения безопасности. С другой стороны, решение вопросов безопасности бизнеса должно быть согласовано с обеспечением безопасности государства и общества в целом, не противоречить обеспечению индивидуальной (личной) безопасности.

Другой проблемой является наличие противоречий между обеспечением различных видов безопасности, в том числе международной и национальной, личности и государства. Хотя, например, ООН настаивает, что безопасность человека не подменяет безопасность государств и не отменяет основополагающего принципа суверенитета, а, наоборот, основана на национальной ответственности [Доклад по безопасности человека …, 2013, с. 4]. Тем не менее различные подходы к безопасности не только существуют в разных странах, в разных научных дисциплинах и у разных специалистов, но и регулярно проявляются в практической деятельности.

Однако сегодня «угрозы и опасности приобрели общепланетный характер и масштаб, и уже невозможно выйти из общецивилизационного кризиса без широкого использования новых способов и механизмов обеспечения безопасности» [Урсул, 2018, с. 13, 14]. Многие специалисты согласны с тезисом о неразрывной взаимосвязи безопасности и современного развития (в контексте его устойчивости), необходимости определенного соотношения (меры) между ними в рамках общего подхода.

Созданию общей теории безопасности во многом препятствуют институциональные барьеры в научной сфере (в том числе границы между различными дисциплинами и научными организациями), которые мешают выявлению связей и взаимозависимостей различных видов безопасности. Недостаточная проработанность общей теории безопасности, в свою очередь, обусловливает фрагментарность учебного курса «безопасность жизнедеятельности» и низкую прогностичность научных знаний по вопросам безопасности.

В настоящее время уже появились и действуют различные коммерческие и государственные структуры, занимающиеся комплексными вопросами безопасности (в дополнении к традиционным) – ситуационные центры, центры мониторинга, центры прогнозирования и т.д. Однако до создания комплексной системы безопасности на национальном или региональном уровне, т.е. интегрированной системы, которая включает в себя контроль и мониторинг опасностей, а также совокупность организационных, правовых, программно-аппаратных, инженерно-технических и силовых мер, методов и средств, направленных на обеспечение безопасности и соответствующих приоритетам общественного развития, еще далеко. Тем более что такая система должна быть гибкой и способной адаптироваться к возникающим новым явлениям или процессам. Одним из таких процессов, который требует значительного пересмотра сложившихся представлений о безопасности, в настоящее время является цифровизация.

## Цифровизация и ее влияние

Цифровизация, как новый термин, описывающий новое явление, появился во второй половине 1990-х годов, но стал активно использоваться начиная с 2010-х. И, как в случае со многими другими понятиями, для него характерно разнообразие подходов, определений и взглядов.

В узком (технологическом) смысле процесс цифровизации можно представить как переход на цифровой способ связи, т.е. запись и передачу данных с помощью цифровых устройств. В этой трактовке он выступает как очередной этап процесса автоматизации, открывающий новые возможности: автоматизации не только физических действий, но и некоторых интеллектуальных функций; комбинирования и сочетания различных новых ИКТ (датчиков, программ и т.д.); организации взаимодействия разнообразных цифровых устройств между собой (без участия человека) посредством запрашивания и предоставления данных. На этой основе возникают и распространяются новые технические решения, в том числе безлюдные технологии и робототехника, комплексные платформы («умные» системы и устройства), Интернет вещей (IoT – Internet of things), 3D-печать и т.д. Происходящие изменения во многом аналогичны преобразованиям, обусловленным процессом электрификации в начале XX в.

В широком смысле процесс цифровизации означает переход к системе экономических, социальных и культурных отношений, основанных на использовании новых ИКТ [Митин, 2017]. Циф-

ровые технологии проникают во все сферы общества, в связи с чем можно говорить о его цифровой трансформации и о двух параллельных (хотя и взаимосвязанных) направлениях преобразований. Первое является, прежде всего, социальным и выражается в формировании новой социальной среды за счет развития новых способов коммуникаций и конструкций виртуального мира – так называемого Интернета людей (IoP – Internet of people). В этот процесс входит оцифровка научного и культурного наследия (создание электронных библиотек, музеев и изданий); проведение общественных мероприятий онлайн (онлайн-трансляции, веб-конференции и прочее); распространение социальных сетей, наконец, конструирование электронного государства. В этом контексте можно говорить об искусственном процессе создания ноосферы, о которой писал еще В.И. Вернадский. Новая (цифровая) социальная среда неизбежно ведет к психофизическим изменениям самого человека и к серьезному преобразованию всего общества. Второе направление трансформации захватывает преимущественно экономическую и финансовую сферы, а также управление, и заключается в формировании так называемой цифровой экономики – появлении новых видов деятельности, продуктов и услуг (создание новой стоимости), новых моделей бизнеса, модернизации традиционных отраслей на основе использования цифровых технологий [Положихина, 2018, с. 11–12].

Очевидно, что разные трактовки процесса цифровизации в основном обусловлены различиями в методологии разных научных дисциплин. Сближение подходов возможно на основе применения общенаучных методов. Например, использование системного подхода и некоторых положений теории информации позволяют создать упрощенную модель цифровизации с точки зрения влияния новых (цифровых) технологий на социально-экономические объекты (рис. 2).


**Рис. 2. Влияние процесса цифровизации на функционирование открытой системы**

Любой социально-экономический объект (личность, сообщество, организацию) можно представить в виде информационно открытой системы – «черного» (если внутренние процессы внешнему наблюдателю неизвестны) или «белого» (когда внутренние процессы внешнему наблюдателю понятны) ящика, обменивающегося информацией с другими системами и внешней средой.

Функционирование такой системы включает следующие этапы: поступление внешней (входящей) информации или данных; переработка этой информации (данных); передача вновь созданной (исходящей) информации (данных) другим системам или во внешнюю среду.

В настоящее время доля внешней информации (данных), поступающей в социально-экономические системы (объекты) в преобразованной (цифровой) форме, непрерывно растет (Интернет, онлайн-издания и т.д.). Переработка информации в этих системах также во все большей степени осуществляется с применением цифровых технологий (искусственный интеллект, виртуальная и дополненная реальность, машинное обучение и т.п.). Наконец, способы коммуникации, связи и передачи информации (данных) все больше основываются на цифровых технологиях (мобильные устройства, социальные сети и т.д.). Таким образом, использование новых (цифровых) технологий оказывает системное влияние на функционирование социально-экономических объектов (информационно открытых систем).

Одни специалисты с энтузиазмом относятся к процессу цифровизации, видя в нем основной тренд современного общественного развития. Скептики считают его очередным модным термином (хотя и более удачным, чем предыдущие), с помощью которого пытаются описать наблюдаемую непростую реальность. Но как бы то ни было, нельзя игнорировать радикальные отличия мира «до и после Интернета», а также то, насколько новые ИКТ «вписаны» в современную действительность.

«Цифровые технологии вышли за пределы информационных процессов, проникли в материально-вещественные технологии и вступают во взаимодействие с “аналоговыми технологиями” органического мира… наука столкнулась с необходимостью понимания и интерпретации аналого-цифрового дуализма», присущего современному обществу [Кефели, Колбанев, 2018, с. 218]. И с этой идеей трудно не согласиться.

Необходимо иметь в виду, что процесс цифровизации еще продолжает развиваться, а социум находится только в начальной стадии трансформации и формирования новых общественных отношений. При этом «мы еще очень мало знаем сами о себе»: как о функционировании и особенностях человеческой психики, сознания и подсознания [Колин, Урсул, 2015, с. 268], так и об общественном развитии в целом. В связи с этим динамичный процесс цифровизации вызывает много опасений.

## Риски цифровизации

Развитие и распространение новых ИКТ приносит очевидную пользу бизнесу, человеку и обществу в целом. Однако уже очевидны и негативные последствия цифровизации. Всемирный банк в докладе 2016 г. выделил следующие риски*:* киберопасность; возможность массовой безработицы; рост «цифрового разрыва» (разрыв в цифровом образовании, в условиях доступа к циф-

ровым услугам и продуктам и, как следствие – разрыв в уровне благосостояния) между гражданами и бизнесами внутри стран, а также между странами [Доклад о мировом развитии …, 2016, с. 18]. Многочисленные работы, посвященные теме цифровизации общества и развитию цифровой экономики, значительно расширили этот список. При этом специалисты из разных научных дисциплин акцентируют внимание на различных вызовах безопасности.

В связи с этим очевидно желание систематизировать риски и угрозы, возникающие или обостряющиеся благодаря процессу цифровизации. Результаты попытки, предпринятой автором, представлены в табл. 4.

Таблица 4

**Виды рисков и угроз безопасности, связанные с процессом цифровизации***

| № пп | Представления о цифровизации | Виды безопасности | Риски и угрозы | Объект |
|---|---|---|---|---|
| 1. | Технико--экономический процесс | Технологическая, экономическая, финансовая | Уязвимость новых систем (быстрорастущ сложность, возможность технологических сбоев);<br>Разработка и распространение проблемных инноваций;<br>Рост потребления электроэнергии;<br>монопольное использование новых технологий;<br>исчезновение или сжатие традиционных рынков;<br>Недостаточное регулирование (лакуны) новых рынков и видов деятельности;<br>Интернет-пиратство и нарушения авторских прав;<br>Разглашение коммерческой тайны;<br>Новые виды промышленного шпионажа;<br>Кибероружие;<br>цифровое неравенство;<br>Негативные изменения на рынке труда (снижение уровня социальной защищенности, нестабильность занятости, безработица) | Бизнес, государство, общество |
| 2. | Социально-культурный процесс | Социальная, культурная, личностная, общественная | Загрязнение информационного пространства;<br>Доступ детей к опасной информации или контактам;<br>Прозрачность частной жизни;<br>Недостаточная защита персональных данных;<br>Киберпреступность;<br>Изменения в психике («компьютерная зависимость») и модели поведения (потеря способности к межличностному общению);<br>Клиповость сознания (сокращение возможностей долговременной памяти, способности к концентрации внимания и глубокому анализу);<br>Виртуализация действительности (снижение степени ответственности и гуманизма);<br>Фрагментация социума;<br>Возможность навязывания продукта, в том числе политического;<br>Ослабление демократических начал в управлении | Личность, общество |
| 3. | Процесс преобразования информации | Информационная, технологическая | Манипулирование данными (спам и др.);<br>Нарушение процессов переработки и хранения информации (вирусы, потеря информации, нарушение ее целостности и конфиденциальности и т.д.);<br>Влияние на средства коммуникации и связи (несанкционированный доступ, использование электронной почты или мобильных устройств неизвестными лицами и т.п.) | Личность, бизнес, государство |

* Составлена автором на основе литературных источников.

Безусловно, приведенный перечень опасностей не является исчерпывающим. Но даже он показывает, что цифровая безопасность шире информационной, а наибольшее количество ее рисков связано с человеческим фактором и качеством человеческого капитала. И этим она принципиально отличается от информационной безопасности (табл. 3 и 4).

«Изменяя мир, человек сам становится другим» [Колин, Урсул, 2015, с. 268]. Данные обстоятельства определяют возрастание значения социальных наук в решении вопросов безопасности.

## Обеспечение цифровой безопасности

Самым очевидным и простым направлением обеспечения цифровой безопасности является увеличение расходов на информационную безопасность и соответствующую инфраструктуру как бизнеса, так и стран в целом. Уже в конце 1980-х годов в разных странах мира появились государственные и корпоративные центры мониторинга и оперативного реагирования на инциденты информационной безопасности. Во многих компаниях существуют собственные соответствующие подразделения. В 2017 г. в России был утвержден Федеральный закон о безопасности критической информационной инфраструктуры № 187-ФЗ от 26.07.2017. С 2018 г. начала действовать ГосСопка – государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак.

По мнению Всемирного банка, развитие цифровой экономики требует определенных аналоговых дополнений, в том числе: нормативно-правовой базы, обеспечивающей высокий уровень конкуренции; навыков населения, позволяющих использовать новые технологии; подотчетных институтов [Доклад о мировом развитии …, 2016. с. 8, 29]. «Обществу еще предстоит справиться с нарастающими опасениями негативных последствий цифровизации… При ответе на эти вызовы на первый план выходят задачи регулирования цифровой экономики», – считают специалисты НУИ ВШЭ [Что такое цифровая экономика …, 2019, с. 5].

Некоторые ученые рассматривают вопросы обеспечения безопасности в более широком контексте. По мнению С.Ю. Глазьева, необходимо инициировать разработку наднациональных правовых актов в области нейтрализации угроз, стоящих перед человечеством. Ограничительные меры должны включать: 1) запрет на клонирование людей; 2) запрет на создание опасных и болезнетворных вирусов, иных форм биологического оружия; 3) внедрение международных стандартов вживления в организм человека кибернетических устройств; 4) мониторинг искусственного интеллекта для выявления потенциально опасных созданных систем; 5) унифицированную сертификацию специалистов в области ИКТ; 6) разработку международных технических регламентов и процедур сертификации роботов-андроидов [Глазьев, 2017]. Представляется, что такие направления обеспечения безопасности во многом актуальны и для национального уровня.

Процесс цифровизации в значительной степени затрагивает сферу образования и рынок труда, связан с появлением новых и отмиранием ряда традиционных профессий. Вопрос кадров – кто будет разрабатывать, производить и использовать новую технику, – становится приоритетным с точки зрения распространения новых технологий. Избежать массовой безработицы и удовлетворить потребности в новых компетенциях возможно за счет прогнозирования и планирования спроса на трудовые ресурсы, а также внедрения образовательных программ, которые касались бы не только подготовки новых специалистов, но и переподготовки старых. Причем масштаб цифровой трансформации, сопоставимый с новой индустриализацией, определяет существенное увеличение затрат на обучение и переобучение кадров.

Наконец, минимизация возможных негативных последствий требует оценки безопасности новых технологий еще на стадии их создания [Иванов, Малинецкий, 2017, с. 53–54]. В связи с этим специалисты предлагают ввести социогуманитарную экспертизу планирования и внедрения новых (в том числе цифровых) технологий.

Следует признать, что для обеспечения цифровой безопасности, помимо формальных или формализованных методов, нужны еще неформальные регуляционные механизмы – прежде всего, выработка определенных принципов цифровой культуры. Специалисты считают, что глобальная цифровизация с неизбежностью ведет к формированию новой культуры, весьма агрессивной по отношению к традиционной, и ее распространению во всем мире. Одновременно должна создаваться и новая этика – этика цифрового мира, с соответствующими моральными ограничениями и нравственными императивами. Определенные принципы поведения в цифровом мире должны стать такими же обязательными как, например, соблюдение тайны переписки для работников обычной почты [Колин, Урсул, 2015, с. 265, 267].

С 2006 г. в России действует Федеральный закон о защите персональных данных № 152-ФЗ от 27.07.2006. Однако отношение к этому вопросу, прежде всего, со стороны самих граждан недостаточно серьезное. Люди с удивительным легкомыслием выкладывают в Интернет массу информации о себе и слабо защищают применяемые устройства (программы). Специалисты подчеркивают, что многие проблемы в сфере информационной безопасности возникают из-за недостаточно ответственного поведения пользователей [Удалов, 2018, с. 13]. Особую остроту вопросы защиты информации и данных приобретают в условиях организации дистанционной (удаленной) работы сотрудников, использования новых финансовых технологий и цифровых моделей бизнеса. Цифровая трансформация общества подразумевает развитие не только цифровой грамотности, т.е. умения пользоваться новыми ИКТ и цифровыми продуктами или услугами, но и цифровой гигиены, т.е. знаний о том, что делать не следует.

Цифровая культура должна стать частью современной культуры безопасности жизнедеятельности или системы табу и ограничений, описывающей риски и угрозы выхода за пределы безопасности [Пименов, 2019, с. 59]. Вместе с тем нельзя не признавать существование деструктивной контркультуры, прямо противоположной культуре безопасной жизнедеятельности. В связи с этим необходимо уделять особое внимание воспитанию необходимых культурных навыков (принципов, ценностей, моделей поведения) в системе образования. Особенно важно сформировать адекватные культурные представления в молодежной среде – тем поколениям, которые будут жить в создаваемом сейчас цифровом мире.

## Заключение

Представления о безопасности, возникнув вместе с появлением человеческого общества, изменяются в соответствии с общей эволюцией взглядов на общество, государство и личность. Хотя существует и национальная специфика подходов (например, в России) вследствие особенностей исторического развития. Главные направления преобразований связаны со значительным расширением представлений о безопасности и повышением внимания к невоенным (несиловым) аспектам. Одновременно предпринимаются попытки создания общей теории безопасности, направленные на то, чтобы согласовать безопасное и устойчивое развитие, учесть влияние новых явлений и процессов.

В настоящее время по сравнению с началом 1990-х годов научный интерес к теме безопасности в общественных дисциплинах значительно вырос, изменилась структура информационного потока. Фиксируемое увеличение количества экономических, социологических, культурологических и философских работ отечественных авторов, связанных с проблемами безопасности, отражает определенное смещение приоритетов. Хотя интенсивность внимания к вопросам безопасности продолжает различаться как по отдельным социальным наукам, так и по разным временным отрезкам. Преобладающая рефлексия на уже свершившиеся события свидетельствует о крайне низкой степени прогностичности имеющихся научных знаний по данному направлению. В значительной степени это определяется недостаточной проработанностью общей теории безопасности, в том числе недоучетом связей между различными ее аспектами.

Продолжающие существовать различия во взглядах на безопасность (включая разнообразные определения терминов) и резкий рост количества выделяемых частных видов безопасности обусловливает потребность в выработке общего подхода к этим вопросам. Общая теоретическая основа необходима для создания комплексной системы обеспечения безопасности (достаточно гибкой по отношению к возникающим новым явлениям или процессам), а также для совершенствования соответствующих учебных курсов.

Одним из процессов, адаптироваться к которому должна как теория безопасности, так и системы по обеспечению безопасности, является цифровизация. Этот динамичный процесс, в результате которого меняется не только окружающая среда, но и сам человек и общество в целом, ожидаемо вызывает много опасений. Проведенное исследование показывает, что использование новых (цифровых) ИКТ оказывает системное воздействие на функционирование социально-экономических объектов, выступающих в качестве информационно открытых систем. В связи с этим цифровая безопасность представляется шире информационной. Причем наибольшее количество рисков цифровизации связано с человеческим фактором и качеством человеческого капитала.

Данные обстоятельства обусловливают возрастание значения социальных наук в решении вопросов безопасности, а также необходимость сочетания формальных и неформальных способов регулирования для обеспечения безопасности. При этом не следует забывать, что процесс цифровизации еще продолжает развиваться, а социум находится только в начальной стадии трансформации и формирования новых общественных отношений.

Нельзя не согласиться с утверждением, что «надо знать особенности нашего “цифрового” времени, изучать их и вырабатывать меры по снижению рисков и максимальному использованию преимуществ» [Гилинский, 2018, с. 189]. Именно в этом заключается цель разработки общей теории безопасности и создаваемой на ее основе комплексной системы обеспечения безопасности. Причем положения теории безопасности должны быть вписаны в общую стратегию развития страны (бизнеса), а принципы обеспечения комплексной безопасности – стать органичной частью поведения разных субъектов – от отдельного человека до общества в целом.

## Список литературы

*Варшавский А.Е.* Основные проблемы реализации четвертой промышленной революции в России // Производство, наука и образование России: технологические революции и социально-экономические трансформации: сб. материалов V Международного конгресса (ПНО- V) / под общ. ред. С.Д. Бодрунова. – Москва: ИНИР им. С.Ю. Витте, 2019. – С. 95–105.

Геополитика и национальная безопасность: словарь основных понятий и определений / под ред В.Л. Манилова. – Москва, 1998. – 254 с.

*Гилинский Я.И.* Девиантность в цифровом мире // Проблемы деятельности ученого и научных коллективов: международ. ежегодник / ИИЕТ РАН. – Санкт-Петербург, 2018. – № 4(34). – С. 182–190.

*Глазьев С.Ю.* Великая цифровая революция: вызовы и перспективы для экономики XXI века // AURORA.NETWORK. Глазьеврy. Публикации. Экономика. – 2017. – 14.09. – URL: https://glazev.ru/articles/6-jekonomika/54923-velikaja-tsifrovaja-revoljutsija-vyzovy-i-perspektivy-dlja-jekonomiki-i-veka%20glazev.ru (дата обращения 01.03.2020.)

Доклад о мировом развитии 2016. Цифровые дивиденды: обзор / Всемирный банк. – Вашингтон, 2016. – 58 с.

Доклад по безопасности человека Генерального секретаря ООН / ООН. Генеральная ассамблея. – 2013. – 23.12. – 25 с. – URL: https://www.unocha.org/sites/dms/HSU/S-G%20Report%20on%20Human%20Security%20A.68.685%20%28Russian%29.pdf (дата обращения 15.03.2020)

*Дьяченко О.В.* Дефиниция категории «цифровая экономика» в зарубежной и отечественной экономической науке // Экономическое возрождение России. – Санкт-Петербург, 2019. – № 1(59). – С. 86–98.

Закон РФ «О безопасности» от 05.03.1992 № 2446–1 (не действ.) // Ведомости СНД и ВС РФ. – Москва, 1992. – № 15. – Ст. 769.

*Иванов В.В., Малинецкий Г.Г.* Цифровая экономика: мифы, реальность, перспективы. – Москва: РАН, 2017. – 63 с.

*Кефели И.Ф., Колбанев М.О.* Асфацефотроника – наука глобальной безопасности в эпоху антропоцена // Перспективные направления развития отечественных информационных технологий: Материалы IV Международной конференции, Севастополь, 18–22 сентября 2018 г. / науч. рук. Б.В. Соколов. – Севастополь, 2018. – С. 216–219.

Концепция общественной безопасности (утв. Президентом РФ от 14.11.2013 № Пр-2685) // КонсультантПлюс. – Москва, 2013.

*Колин К.К., Урсул А.Д.* Информация и культура. Введение в информационную культурологию. – Москва: Изд-во «Стратегические приоритеты», 2015. – 288 с.

*Кульков В.М.* Противоречивое влияние цифровизации на социально-экономическое развитие // Производство, наука и образование России: технологические революции и социально-экономические трансформации: сб. материалов V Международного конгресса (ПНО- V) / под общ. ред. С.Д. Бодрунова. – Москва: ИНИР им. С.Ю. Витте, 2019. – С. 353–359.

*Лазар М.Г.* Цифровизация общества, ее последствия и контроль над населением // Проблемы деятельности ученого и научных коллективов: международ. ежегодник / ИИЕТ РАН. – Санкт-Петербург, 2018. – № 4(34). – С. 170–181.

*Митин В.* Семь определений цифровой экономики // CRN ИТ-бизнес. Новости. – Москва, 2017. – URL: https://www.crn.ru/news/detail.php?ID=116780 (дата обращения 12.03.2020.)

*Митяева Н.В., Заводило О.В.* Барьеры цифровой трансформации и пути их преодоления // Вестник Саратовского гос. соц.-эконом. ун-та (филиал РЭУ им. Г.В. Плеханова). – Саратов, 2019. – № 3 (77). – С. 20–24.

*Пименов Н.А.* Культура безопасности жизнедеятельности как условие безопасности личности и общества // Актуальные вопросы безопасности жизнедеятельности в современных условиях: сб. ст. / Фин. ун-т при Правительстве РФ. – Москва: Объединенная редакция, 2019. – С. 54–63.

*Положихина М.А.* Цифровая экономика как социально-экономический феномен // Экономические и социальные проблемы России: сб. науч. трудов / РАН. ИНИОН. Центр социал. науч.- информ. исслед. Отд. экономики; ред. кол.: Макашева Н.А., гл. ред., и др. – Москва, 2018. – № 1: Цифровая экономика: состояние и перспективы развития / сост. вып. Положихина М.А. – С. 8–38.

*Скляр М.А., Кудрявцева К.В.* Цифровизация: основные направления, преимущества и риски // Экономическое возрождение России. – Санкт-Петербург, 2019. – № 3(61). – С. 103–126.

*Удалов Д.В.* Угрозы и вызовы цифровой экономике // Экономическая безопасность и качество. – Саратов, 2018. – № 1(30). – С. 12–18.

Указ Президента РФ от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации» // Собрание законодательства РФ. – Москва, 2016. – № 1, ч. 2. – Ст. 212.

Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства РФ. – Москва, 2016. – № 50. – Ст. 7074.

Указ Президента РФ от 13.05.2017 № 208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года» // Собрание законодательства РФ. – Москва, 2017. – № 20. – Ст. 2902.

Указ Президента РФ от 06.05.2018 № 198 «Об Основах государственной политики Российской Федерации в области промышленной безопасности на период до 2025 года и дальнейшую перспективу» // Собрание законодательства РФ. – Москва, 2018. – № 20. – Ст. 2815.

Указ Президента РФ от 13.05.2019 № 216 «Об утверждении Доктрины энергетической безопасности Российской Федерации» // Собрание законодательства РФ. – Москва, 2019. – № 20. – Ст. 2421.

Указ Президента РФ от 21.01.2020 № 20 «Об утверждении Доктрины продовольственной безопасности Российской Федерации» // Собрание законодательства РФ. – Москва, 2020. – № 4. – Ст. 345.

*Урсул А.Д.* Безопасность и развитие: междисциплинарный подход и глобальное измерение // Альтернативные модели глобализации и проблемы современной глобальной динамики. – Ростов-на-Дону, 2018. – С. 13–32.

Федеральный закон от 10.01.2002 № 7-ФЗ «Об охране окружающей среды» // Собрание законодательства РФ. – Москва, 2002. – № 2. – Ст. 133.

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. – Москва, 2006. – № 31, ч. 1. – Ст. 3448.

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // Собрание законодательства РФ. – Москва, 2006. – № 31, ч. 1. – Ст. 3451.

Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности» // Собрание законодательства РФ. – Москва, 2011. – № 1. – Ст. 2.

Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры» // Собрание законодательства РФ. – Москва, 2017. – № 31, ч. 1. – Ст. 4736.

Что такое цифровая экономика? Тренды, компетенции, измерение: докл. к XX Апр. междунар. науч. конф. по проблемам развития экономики и общества, Москва, 9–12 апр. 2019 г. / Г.И. Абдрахманова, К.О. Вишневский, Л.М. Гохберг и др.; науч. ред. Л.М. Гохберг; НИУ ВШЭ. – Москва: Изд. дом Высшей школы экономики, 2019. – 82 с.

New Dimensions of Human Security: Human Development Report 1994 / UNDP. – New York; Oxford: Oxford University Press, 1994. – 226 p.

# УСТОЙЧИВОЕ РАЗВИТИЕ В УСЛОВИЯХ НОВЫХ ВЫЗОВОВ

**Стрижов Станислав Алексеевич**

Доктор экономических наук, профессор, заведующий кафедрой инновационных технологий в государственной сфере и бизнесе Института бизнеса и делового администрирования Российской академии народного хозяйства и государственной службы при Президенте РФ (Москва, Россия)

***Аннотация.*** *Статья посвящена актуальной проблеме обеспечения устойчивого развития РФ в условиях новых вызовов. Рассматривается ситуация в стране, связанная с реакцией на пандемию коронавируса COVID-19, анализируется роль цифровых технологий в смягчении ее влияния на социум. Высказывается мнение о том, что вызванные пандемией изменения ведут к необходимости пересмотра некоторых приоритетов в рамках глобальных целей и задач устойчивого развития.*

***Ключевые слова:*** *устойчивое развитие; цели устойчивого развития; цифровизация; пандемия коронавируса; система здравоохранения*

**Для цитирования:** Стрижов С.А. Устойчивое развитие в условиях новых вызовов // Социальные новации и социальные науки. – Москва: ИНИОН РАН, 2020. – № 1. – С. 28–36.

URL: https://sns-journal.ru/ DOI: 10.31249/snsn/2020.01.02

## Введение

Переход к XXI в. человечество встретило в достаточно сложной ситуации. Вопреки ожиданиям, стремительный технологический рывок и бурный экономический рост не привели к решению многих острых социально-экономические проблем: глобальных масштабов нищеты и безработицы; неравенства внутри отдельных стран и между ними; угроз здоровью и жизни людей, обусловленных как природными и техногенными факторами, так и различного рода гуманитарными кризисами; ухудшения экологии и изменения климата.

Поиск путей выхода из создавшегося положения привел к формированию представлений об устойчивом развитии как основе того, каким должно быть будущее. В опубликованном в 1987 г. Международной комиссией по окружающей среде и развитию первом концептуальном документе – докладе «Наше общее будущее» – было дано следующее определение: «*…устойчивое и долговременное развитие представляет собой не неизменное состояние гармонии, а скорее процесс изменений, в котором масштабы эксплуатации ресурсов, направление капиталовложений, ориентация технического развития и институционные изменения согласуются с нынешними и будущими потребностями*» [Наше общее будущее]. Новая стратегия развития цивилизации исходит не из приоритетов сегодняшнего дня, а ставит нынешнее и будущее поколения на одну ступень, приравнивая их по возможностям удовлетворения жизненных потребностей (принцип равенства возможностей развития поколений).

В сентябре 2015 г. в Нью-Йорке 193 государства – члена ООН (в том числе Россия) единогласно приняли новую Повестку дня в области устойчивого развития – глобальную программу по обеспечению устойчивого будущего. Были сформулированы 17 Целей устойчивого развития (ЦУР) до 2030 г., касающиеся климата, социальных и экономических проблем (рис. 1).

Сегодня устойчивое развитие связывают именно с этими целями, а поиск оптимальных путей их достижения рассматривается как ключевая задача в глобальном и национальном масштабах.

Основные направления устойчивого развития нашли отражение в современных реформах социального и экологического законодательства РФ, включая различные государственные программы и проекты в области демографии, борьбы с бедностью, образования, здравоохранения и экологии, а также в различных инициативах гражданского общества и в новых бизнес-практиках. В то же время в основных документам стратегического планирования тема устойчивого развития в ее комплексном выражении, начиная с самих понятий «устойчивое развитие», «социальная ответ-

ственность государства», «зеленая экономика», представлена недостаточно четко [Стрижов, Коданева, 2019].


**Рис. 1. Цели ООН в области устойчивого развития**

Следует отметить, что отдельные аспекты устойчивого развития, отраженные в ЦУР, находятся в поле зрения высшего руководства страны. Так, в Послании Президента РФ Федеральному собранию 2018 г. было уделено серьезное внимание экологическим проблемам [Послание Президента РФ, 2018]. Актуализация решения задач ЦУР в России нашла отражение и в майском указе Президента РФ 2018 г. [Сахаров, Колмар, 2019].

Следует согласиться с мнением о том, что, когда разрабатывались ЦУР, предполагалось, что мировая экономика будет стабильно расти [Antoniades, Widiarto, Antonarakis, 2019]. Эксперты учитывали негативное влияние на экономику финансовых кризисов, вносящих коррективы в возможность достижения тех или иных целей устойчивого развития. Однако они не могли даже предположить, с какими новыми угрозами столкнется не только мировая экономика, но в первую очередь безопасность людей в планетарном масштабе в XXI в.

## Вызовы пандемии

Безусловно, мировое сообщество всегда уделяло внимание угрозе возникновения эпидемий инфекционных заболеваний. Но в последние годы они, как правило, носили локальный, очаговый характер. Поэтому считалось, что национальные системы здравоохранения способны с ними справляться, а развитие здравоохранения в данном направлении не является приоритетной задачей. Возможно, именно по этой причине в Докладе «Наше общее будущее» системы здравоохранения обойдены вниманием.

Пандемия коронавируса COVID-19 стала новым вызовом современности, в каком-то смысле крайне эгалитарным, подчеркивающим равенство людей перед лицом существующей опасности.

Борясь с распространением инфекции, мир одновременно погружается в самый глубокий со времен Великой депрессии 1930-х годов социально-экономический кризис. По оценкам аналитиков JP Morgan Chase & Co, пандемия коронавируса лишит мировую экономику в ближайшие два года 5,5 трлн долл. Эта сумма превышает годовой объем производства товаров и услуг Японии [Bloomberg оценил …, 2020]. Всемирная торговая организация (ВТО) ожидает, что объем мировой торговли сократится в 2020 г. на 13–32% из-за нарушения нормальной экономической активности и жизни во всем мире. Спад текущего года может превысить масштабы сокращения торговли, наблюдавшиеся в 2008–2009 годах в период глобального финансового кризиса [Bloomberg оценил …, 2020]. В первую очередь кризис затрагивает рынок труда.

Эксперты Центра макроэкономического анализа и долгосрочного прогнозирования считают, что к концу апреля текущего года без работы, под риском увольнения или сокращения заработка могут остаться 10 млн россиян. В худшем случае по итогам года уровень безработицы вырастет в России до 6%, а в следующем году, если кризис продолжится, то и до 6,7% [Десять миллионов …, 2020]. По мнению председателя Счетной палаты А. Кудрина, в период этого кризиса в России число безработных увеличится с 2,5 млн до 8 млн человек [Кудрин …, 2020].

В данной ситуации перед мировым сообществом в целом и Россией в частности правомерно поставить вопрос не о достижении ЦУР в ближайшем будущем, а о возврате на утраченные в результате жесткого кризиса позиции. При этом речь следует вести и о пересмотре целей устойчивого развития. Развитие здравоохранения должно быть определено в качестве приоритетной цели устойчивого развития с соответствующей корректировкой задач, которые были ранее обозначены в рамках ЦУР-3.

Данная позиция аргументируется прежде всего тем, что локальная эпидемия коронавируса переросла в пандемию именно из-за неготовности систем здравоохранения большинства государств, в том числе и России, вовремя и результативно среагировать на распространение инфекции. Фактически COVID-19 стал фактором проверки эффективности национальных систем здравоохранения.

## Проблемы функционирования отечественной системы здравоохранения

Можно констатировать, что эпидемия коронавируса наглядно продемонстрировала недостатки реформы отечественного здравоохранения. Власти не усвоили урок пандемии свиного гриппа, который показал, как легко инфекции могут распространяться по всему миру.

Ради выполнения майских указов Президента РФ о повышении средней зарплаты в здравоохранении Минздрав пошел по пути сокращения среднего и младшего медперсонала. По данным

Росстата, в период с 2013 по 2019 г. количество младших медработников сократилось в 2,6 раза, среднего персонала – на 9,3%, врачей – на 2% [Готово ли …, 2020], инфекционистов-эпидемиологов – на 31,8% (рис. 2).


**Рис. 2. Динамика сокращения численности врачей-эпидемиологов [Готово ли …, 2020]**

Почти в 2,4 раза сократилось и число коек инфекционного профиля – со 140 тыс. в 1990 г. до 59 тыс в 2018 г. (рис. 3). Только в Москве с 2011 г. ликвидировано почти 2,2 тыс. из 4,8 тыс. койко-мест. 3-ю инфекционную больницу в Печатниках на 570 мест в 2015 г. власти решили перестроить в производственно-складской комплекс [Готово ли ..., 2020]. В случае функционирования данной больницы был бы выигрыш как во времени для лечения заболевших коронавирусом, так и с точки зрения экономии бюджетных средств, поскольку отпала бы необходимость строить новый инфекционный комплекс.


**Рис. 3. Динамика изменения числа коек в инфекционных отделениях, больницах [Готово ли …, 2020]**

Следует отметить, что, сознавая серьезность ситуации, высшее руководство РФ приняло оперативные меры для уменьшения распространения коронавируса по территории страны и для лечения заболевших. Однако принимаемые меры сопровождаются возникновением новых проблем. Из-за перепрофилирования больниц под инфекционные отменили госпитализацию и плановые операции у других больных Ограниченное функционирование ряда поликлиник (по крайней мере, в Москве) создает проблемы для граждан, находящихся под текущим медицинским наблюдением [Готово ли ..., 2020]. Соответственно, требуется корректировка управленческих и организационных процессов в системе здравоохранения.

Негативные последствия введения ограничительных мер в связи с коронавирусом для населения, организаций и учреждений социальной сферы и сферы услуг, а также ряда направлений бизнеса могли быть намного более серьезными, если бы в стране в последние годы не осуществлялись системные мероприятия по цифровизации разных сфер жизнедеятельности.

## Использование новых цифровых технологий в период пандемии

Идеология цифровизации российского государства и общества представлена в двух программных документах: Стратегии развития информационного общества в РФ на 2017–2030 гг. и Программе «Цифровая экономика Российской Федерации» [Программа «Цифровая экономика РФ», 2017]. Кроме того, в настоящее время на рассмотрении Правительства РФ находится разработанный Министерством цифрового развития, связи и массовых коммуникаций РФ проект паспорта национального проекта «Цифровая экономика Российской Федерации». Согласно содержанию официальных документов, перспективы улучшения качества жизни российских граждан связываются с широким применением отечественных информационно-коммуникационных технологий, направленных на повышение производительности труда, эффективности производства и конкурентоспособности страны на мировых рынках, обеспечение ее устойчивого и сбалансированного долгосрочного развития.

Вместе с тем эксперты неоднократно отмечали серьезные провалы в реализации национальной программы «Цифровая экономика», возлагая ответственность за них на Министерство цифрового развития, связи и массовых коммуникаций [Спецпредставитель Президента …, 2020]. Однако следует признать, что именно цифровые технологии стали своеобразной «палочкой-выручалочкой» в условиях пандемии коронавируса.

На протяжении последних лет на разных уровнях велись разговоры о цифровизации, удаленной работе, дистанционном образовании, телемедицине и обсуждались различные альтернативы. Нынешняя ситуация не оставляет другого выбора – эти технологии надо внедрять сейчас.

Посредством цифровых технологий осуществляется контроль за соблюдением режима самоизоляции граждан. В онлайн-режиме оформляются соответствующие пропуска и отслеживается

передвижение транспорта. Для разнообразия времяпрепровождения граждан, находящихся в условиях самоизоляции, многие интернет-платформы на бесплатной основе проводят различные мастер-классы и вебинары, предлагаются разные формы онлайн-общения. Практически вся система образования переведена на дистанционный режим.

Сбербанк в течение последних трех лет активно разрабатывал школьную цифровую платформу. Стояла цель разместить ее с 1 сентября 2020 г. в 150 школах, а с 1 сентября 2021 г. – в тысяче школ. За полтора месяца кризиса по просьбе губернаторов и директоров школ Сбербанк развернул данную платформу в двух тысячах школ, и сегодня на ней реально учатся уже 500 тыс. школьников [Греф ..., 2020].

Эксперты считают, что с появлением коронавируса скорость цифровизации экономики возросла в 10 раз [Кодачигов, 2020].

Одной из неотложных задач цифровизации в современных условиях является создание в кратчайшие сроки системы выявления нуждающихся в помощи государства, и на ее основе оказание своевременных мер поддержки оказавшимся в бедственном положении гражданам, представителям малого бизнеса и самозанятым. Другая задача государства состоит в одновременном обеспечении безопасности людей и их занятости. Неудачное выполнение этих функций может привести к тому, что пример Северной Осетии, жители которой выступили против режима самоизоляции, распространится на другие регионы страны с низким уровнем жизни населения. Остановка экономической деятельности ставит под угрозу удовлетворение элементарных потребностей людей, поэтому помощь из федерального центра и от региональных властей не должна запаздывать. К сожалению, уровень ответственности и способности эффективно решать нештатные задачи у руководителей ряда регионов оставляет желать лучшего.

Особо пристальное внимание в условиях пандемии вызывает состояние отечественной медицины. Эта сфера входит в число наиболее подверженных цифровым трансформациям. Во всем мире обсуждаются этические проблемы инженерии генома человека с целью устранения звеньев, ответственных за опасные хронические заболевания; возможности биотехнологий, нейротехнологий, дополненной и виртуальной реальности вмешиваться в физиологию, изменять отношения человека с окружающим миром.

Развитие телемедицины и онлайн-медицины делает услуги в сфере здравоохранения более доступными, особенно для удаленных районов. Однако существуют и определенные риски. Прежде всего, речь идет о доверии пациентов к дистанционным консультациям, а также о способности врачей ставить верные диагнозы, основываясь исключительно на визуальной картинке, полученной посредством онлайн-систем. Кроме того, аккумулирование информации о пациентах на едином портале несет в себе риски для сохранения медицинской тайны и целостности информации в

случае кибератак. В связи с этим требуются серьезные меры по обеспечению кибербезопасности всех задействованных ресурсов [Коданева, 2019].

В научной литературе и хозяйственной практике достаточно часто употребляется понятие «системообразующая отрасль», к числу который относят, например, энергетику. Сейчас пришло время признать, что *здравоохранение является системовлияющей отраслью.* От способности здравоохранения противостоять эпидемиям (а тем более пандемиям), зависит не только успешное функционирование отраслей экономики (в том числе жизнеобеспечивающих), но и сама возможность стабильного и устойчивого развития страны, безопасность жизни и здоровья ее граждан.

Президент РФ признал важность и незаменимость труда медицинских работников. Теперь дело за тем, чтобы этот абсолютно правильный вывод был воспринят как руководство к действию чиновниками всех уровней. Необходимо прекратить оценивать деятельность здравоохранения с позиции экономической эффективности (что началось с приходом к руководству отрасли «эффективных менеджеров» – М. Зурабова и последующих руководителей). Возглавлять медицинскую отрасль должны профессиональные организаторы здравоохранения, понимающие, что главный критерий ее оценки – это социальная эффективность, которая подразумевает обеспечение сохранности здоровья и жизни людей.

## Заключение

Ученые разных стран высказывают предположения о том, что в будущем возможно повторение вирусных атак. Их успешное отражение зависит от того, насколько адекватно и своевременно будут приниматься необходимые меры со стороны государства в тесном взаимодействии с обществом и бизнесом, основанном на взаимном доверии и высокой социальной ответственности.

Нет сомнения в том, что после выхода из кризиса, вызванного пандемией COVID-19, человечество вернется к повестке устойчивого развития. Перспективы отдельных стран и мирового сообщества в целом по-прежнему зависят от решения задач, соответствующих Целям устойчивого развития. Однако последние должны быть скорректированы с учетом происходящих изменений.

## Список литературы

Готово ли российское здравоохранение к борьбе с коронавирусом // Ведомости. – 2020. – 09.04. – URL: https://www.vedomosti.ru/society/articles/2020/04/09/827471-gotovo-rossiiskoe (дата обращения 10.04.2020.)

*Греф Г.* В этот кризис у нас есть уникальный шанс измениться // Lenta.ru.–2020. – 21.04. – URL: https://lenta.ru/articles/2020/04/21/grefinterview/?fm=1 (дата обращения 10.04.2020.)

Десять миллионов россиян могут остаться без работы к концу апреля // News.ru. – 2020. – 10.04. – URL: https://news.ru/economics/desyat-millionov-rossiyan-mogut-ostatsya-bez-raboty-k-koncu-aprelya/ (дата обращения 10.04.2020.)

*Коданева С.И.* Роль органов федеральной власти РФ в обеспечении устойчивого развития государства перед вызовами цифровой экономики // Россия: тенденции и перспективы развития. – М., 2019. – Вып. 14, ч. 2. – С. 298–302.

*Кодачигов В.* Коронавирус ускорил цифровизацию экономики в 10 раз // Ведомости. – 2020. – 12.04. – URL: https://www.vedomosti.ru/technology/characters/2020/04/12/827841-koronavirus-uskoril-tsifrovizatsiyu-ekonomiki?utm_campaign=glavnoezaden13042020&utm_content=827841-koronavirus-uskoril-tsifrovizatsiyu-ekonomiki&utm_medium=email&utm_source=newsletter (дата обращения 10.04.2020.)

Кудрин спрогнозировал рост числа безработных в России в три раза // Ведомости. – 2020. – 13.04. – URL: https://news.mail.ru/economics/41360748/?frommail=1 (дата обращения 10.04.2020.)

Наше общее будущее: Доклад Международной комиссии по окружающей среде и развитию. – URL: http://xn--80adbkckdfac8cd1ahpld0f.xn--p1ai/files/monographs/OurCommonFuture-introduction.pdf (дата обращения 10.04.2020.)

Послание Президента РФ Федеральному Собранию в 2018 г. // Официальный сайт Президента РФ. – URL: http://kremlin.ru/events/president/news/56957 (дата обращения 10.04.2020.)

Программа «Цифровая экономика Российской Федерации». Утверждена Распоряжением Правительства Российской Федерации от 28 июля 2017 года № 1632-р. // Официальный сайт Правительства РФ. – URL: http://government.ru/docs/28653/ (дата обращения 10.04.2020.)

Рынок труда, занятость и заработная плата // Официальный сайт Росстата. – URL: http://rosstat.gov.ru/labor_market_employment_salaries (дата обращения 10.04.2020.)

*Сахаров А.Г., Колмар О.И.* Перспективы реализации Целей устойчивого развития ООН в России // Вестник международных организаций. – М., 2019. – Т. 14, № 1. – С. 189–206.

Спецпредставитель Президента РФ назвал провалом развитие цифровых технологий в стране // ИА ТАСС. – 2020. – 07.04. – URL: https://tass.ru/nacionalnye-proekty/8182313?fbclid=IwAR3BtqMvk1JYOZeD2wO_Lrvbo6QW1L087rrySXo6dcCJ-eOz5cmkRQOLdao (дата обращения 10.04.2020.)

*Стрижов С.А., Коданева С.И.* Реализация концепции устойчивого развития в России: региональный аспект // Экономика: вчера, сегодня, завтра. – М., 2019. – № 9. – С. 97–111.

*Antoniades A., Widiarto I., Antonarakis A.S.* Financial crises and the attainment of the SDGs: an adjusted multidimensional poverty approach // Sustain Sci.–2019. – URL: https://doi.org/10.1007/s11625-019-00771-z (дата обращения 10.04.2020.)

Bloomberg оценил потери мировой экономики от коронавируса в $5 трлн // РБК. – 2020. – 09.04. – URL: https://www.rbc.ru/economics/09/04/2020/5e8ec97f9a79478537a44e47 (дата обращения 10.04.2020.).

# ЦИФРОВИЗАЦИЯ И БЕЗОПАСНОСТЬ: ПРОБЛЕМЫ И РЕШЕНИЯ

**Левашов Виктор Константинович**

Доктор социологических наук, руководитель центра стратегических социальных и социально-политических исследований ИСПИ РАН (Москва, Россия)

**Сарьян Вильям Карпович**

Доктор технических наук, академик НИН РА, профессор МФТИ и МТУСИ (Армения, Россия)

***Аннотация.*** *Стремительное развитие инфокоммуникационной среды поднимает вопросы устойчивого функционирования национальных информационных систем и управления, безопасности человека. На конкретном примере доказывается необходимость администрирования информационно-коммуникационных услуг на базе социотехнологических стандартов и регламентов.*

***Ключевые слова:*** *цифровизация; достоверность информации; средства массовой информации; информационная услуга; администрирование информационных услуг.*

**Для цитирования:** Левашов В.К., Сарьян В.К. Цифровизация и безопасность: проблемы и решения // Социальные новации и социальные науки. – Москва: ИНИОН РАН, 2020. – № 1. – С. 37–46.

URL: https://sns-journal.ru DOI: 10.31249/snsn/2020.01.03

## Введение

Новые информационно-коммуникационные технологии (ИКТ) все в большей степени проникают в разные сферы и направления жизнедеятельности общества и государства, в том числе российского. Сети электросвязи, передающие разнообразную информацию с помощью электрических сигналов по проводам или радиосигналами, трансформируются в единую глобальную конвергентную инфокоммуникационную среду (ИКС) [Бутенко, Назаренко, Сарьян, 2010]. В данном случае представления об ИКС тождественны понятию информационной среды, определенному в «Доктрине информационной безопасности Российской Федерации» (2016) как «совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети “Интернет”, сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений». Предполагается, что инфраструктура ИКС станет ключевым фактором ускорения процесса цифровизации общества, отвечающего задачам его устойчивого развития. ИКС должна объединять физическую инфраструктуру городов, регионов, государств для:

– повышения качества жизни граждан;

– ускорения экономического роста и стимулирования инноваций;

– эффективного и оптимального управления промышленностью, торговлей и другими секторами экономики;

– контроля за экологическим состоянием и снижением негативного воздействия на окружающую среду;

– более быстрого и эффективного предоставления общественных услуг;

– повышения безопасности и конфиденциальности.

Но насколько оправдываются эти ожидания?

Конгломерат стремительно развивающихся цифровых технологий фундаментальным образом изменяет системы социальных, экономических и политических коммуникаций. Во взаимодействии социума и техносферы возникает сложный социотехнологический феномен [Сарьян, Левашов, Назаренко, 2019], позитивные и деструктивные эффекты которого завязываются в узел проблем устойчивого развития общества и государства.

Рост диспаритетов в материальной и духовной сферах обостряет информационное противостояние бедного большинства и богатого меньшинства на планете и в отдельных странах, создает критические степени социально-политических напряжений, которые в условиях кризиса могут привести к самоуничтожению как государства, так и общества. Разнонаправленные национальные социально-политические интересы и возникающие вследствие этого противоречия и дисфункции определяют конфликтный характер функционирования единой глобальной информационной сферы. Ее основные инструменты – средства массовой информации, цифровые социальные и политические коммуникации – находятся под контролем конкурирующих сторон. Сегодня мы наблюдаем и становимся невольными участниками глобальной информационно-технологической конкуренции, в которой сторонники консервации элитарных форм социального управления активно применяют приемы массового манипулирования информацией. Развивающаяся глобальная ИКС поставила и мультиплицировала проблему суверенитета национальных информационных сфер, их безопасного достоверного устойчивого функционирования. Соответственно, информационная безопасность РФ приобрела стратегическое значение.

## Достоверность информации в СМИ

В условиях формирования массовых социальных коммуникаций и объективно востребованного развития институтов гражданских демократий, спекулятивные информационные коммуникации и технологии тормозят формирование достоверных сегментов ИКС (протоноосферы, по Э. Леруа и В.И. Вернадскому) [Вернадский, 1954, с. 673]. Ситуация развивается по сценарию французского философа и социолога Ги Дебора, согласно которому современное общество постепенно становится «обществом спектакля», и впереди нас ждет диктатура массового потребления и тотальных политических репрессий [Дебор, 2000]. Сбудется ли это предсказание потребительского ада фальшивой информационной сферы? Какие уроки необходимо учесть российским ученым и политикам?

Следует признать, что в условиях становления глобального гражданского общества и перехода к массовым цифровым формам публичной демократии ИКС переживает болезнь роста – запаздывание процессов социотехнологических, социополитических и социоправовых трансформаций, – что выражается в нарастающих дисфункциях институтов и средств массовой информации и коммуникации. Американские исследователи F. Gilbert, Th.Petersonand, W. Schramm в середине прошлого века отмечали усиление экономической зависимости печатных и электронных СМИ, а также рост их социальной безответственности [Gilbert, Peterson, Schramm, 1956, p. 78–79]. По их мнению, накопленные в течение десятилетий противоречия в работе либеральных СМИ ведут к деформации института свободной и независимой прессы как в развитых, так и в развивающихся странах.

С одной стороны, СМИ сосредоточили в своих руках огромные властные ресурсы, которые используются ими по собственному усмотрению. Владельцы СМИ тиражируют свои субъективные мнения, особенно в экономических и политических вопросах, дискриминируя мнения оппонентов. В погоне за тиражами и прибылью СМИ часто отдают предпочтение сенсационной и поверхностной информации в ущерб объективной и достоверной. Развлекательность СМИ зачастую оборачивается бессодержательностью. Все чаще СМИ вторгаются в личную жизнь граждан без всяких на то оснований, угрожая своей деятельностью общественной морали или оказывая сопротивление социальным переменам. С другой стороны, во всех развитых странах большинство СМИ, как правило, контролируются крупным капиталом («бизнес-классом»). Для новичков и оппонентов доступ в индустрию СМИ затруднен, в связи с чем свободный и открытый рынок идей, а также распространение достоверной информации оказались под угрозой.

Формирование единой конвергентной ИКС на цифровой технологической платформе привело к тому, что государственные СМИ и средства радио- и телевизионного вещания, которые долгие годы практически монопольно формировали мировоззрение подавляющего большинства граждан своих государств, утратили преимущество территориальной изоляции [Сарьян, 2005]. Это создает широкие возможности для организации информационных войн, так как на любое событие внутри страны или в мире любому абоненту ИКС могут предлагаться прямо противоположные аргументированные оценки. Такие войны могут инициироваться как отдельными группами из бизнес-класса, борющимися за рынки, так и государствами, которые зачастую выполняют их заказы.

Стремление уходящих элит сохранить свое господствующее положение максимально усиливает практики дезинформации. В результате происходит вырождение сущностного качества информации – достоверного отражения действительности, – а СМИ становятся институтом социальной и политической манипуляции. Сегодня функция манипуляции вмонтирована и активно используется в политических технологиях, социальной и коммерческой рекламе с целью заставить граждан совершать политический выбор в интересах корпораций или различных групп политических элит. Такая искаженная информационная сфера по сути своей не отвечает широким общественным потребностям, она социально дисфункциональна.

Масштабные кампании дезинформации выражаются в феномене постправды и сконструированной ложной фейковой информации, состоящей из фрагментов реальных событий, которые перемежаются с вымыслом, слухами, эмоциональными суждениями и мифами. Особенно легко это делать в условиях дозирования информации. Недостоверная информация перестает быть просто феноменом межличностного общения, вырастая в инструментарий информационной сферы социума. Еще недавно в общественном сознании подобная информация воспринималась как недостоверная и сомнительная, но в современных условиях она подается как информация особой, «экс-

клюзивной» достоверности. Манипуляция заменяет социально эффективное управление, дезинформация – информацию, вымысел – правду.

На инфосферу также распространяются рыночные отношения: вымысел, скандалы, мифы и слухи становятся товаром, продаются и покупаются, а их потребительная стоимость зависит от сенсационности. В обществе «спектакля» искусно смоделированные скандалы и сенсации стали инструментами массовых манипуляций эмоциями и поведением в политике, экономике, шоубизнесе и рекламе.

В информационной сфере возникла разновидность симбиоза рекламы и недостоверной информации. Многочисленные рубрики «Эксклюзивная информация», «Скандалы», «Сенсации», «Слухи» в прессе, теле- и радиопередачах, интернет-сайтах, а также рост числа эпатажных блогеров призваны выполнять особую функцию – привлечение внимания пользователей информации к работе конкретного источника информации с целью повышения его рейтинга и, соответственно, росту гонораров от рекламы.

Все вышесказанное значительно снижет безопасность государства и граждан и, к сожалению, хорошо подтверждается событиями, связанными с пандемией, вызванной короновирусом.

Согласно данным опросов Центра стратегических социальных и социально-политических исследований ФГБУН Института социально-политических исследований (ИСПИ) РАН, уже в течение 20 лет граждане достаточно критически оценивают достоверность передач российского радио и телевидения [Экспресс-информация ..., 2019, с. 33]. В 2018 г. лишь 10% респондентов заявляли, что передачи радио и телевидения о событиях и жизни в стране являются правдивыми. Половина опрошенных граждан указывали, что СМИ транслируют поровну достоверную и недостоверную информацию, а 30% считали, что радио и телевидение недостоверно освещают события.

Жители России все меньше доверяют практически всем источникам информации. В 2018 г. граждане считали, что наиболее точно и достоверно отражают информацию Интернет (41%) и центральные СМИ – телевидение (32%) и органы печати (10%). При этом более 30% респондентов затруднились дать ответ. По мнению более половины опрошенных респондентов, радио и телевидение приукрашивают действительное состояние дел. В общественном мнении сформировалась определенная иерархия причин распространения недостоверной информации через СМИ. На первом месте находится «замалчивание событий в средствах массовой информации» (39%), далее – «преднамеренное искажение информации властью, негласная цензура» (38%), «зависимость журналистов от «денежных мешков» (34%), «неискренность политиков» (31%) и «искажение информации журналистами» (29%) [Экспресс-информация ..., 2019, с. 35–37].

России не удалось избежать кризиса информационной сферы. Чуть больше четверти респондентов не доверяют ни одному источнику информации, пятая часть граждан доверяют каналам

межличностного общения, 10% – затруднились ответить на вопрос и только 35% – доверяют СМИ, а 9% – обратятся в случае противоречивости информации к Интернету [Экспресс-информация ..., 2019, с. 38].

Такая ситуация не может не сказываться на ИКС и реализации одного из направления взаимодействия общества и государства – получении гражданами государственных информационных услуг, в том числе услуг, связанных с обеспечением безопасности.

### Инфомационно-коммуникационные услуги и их администрирование

По мере формирования ИКС становится очевидным, что главные критерии ее функционирования – безопасность и достоверность – невозможно обеспечить без эффективного администрирования со стороны государства. Заметим, что в условиях развития пандемии коронавируса большинство государств стало не только осознавать эту потребность, но и решать ее на практике.

На рис. приведена типовая инфраструктура предоставления информационно-коммуникационных (ИК) услуг [Назаренко, Сарьян, 2017].

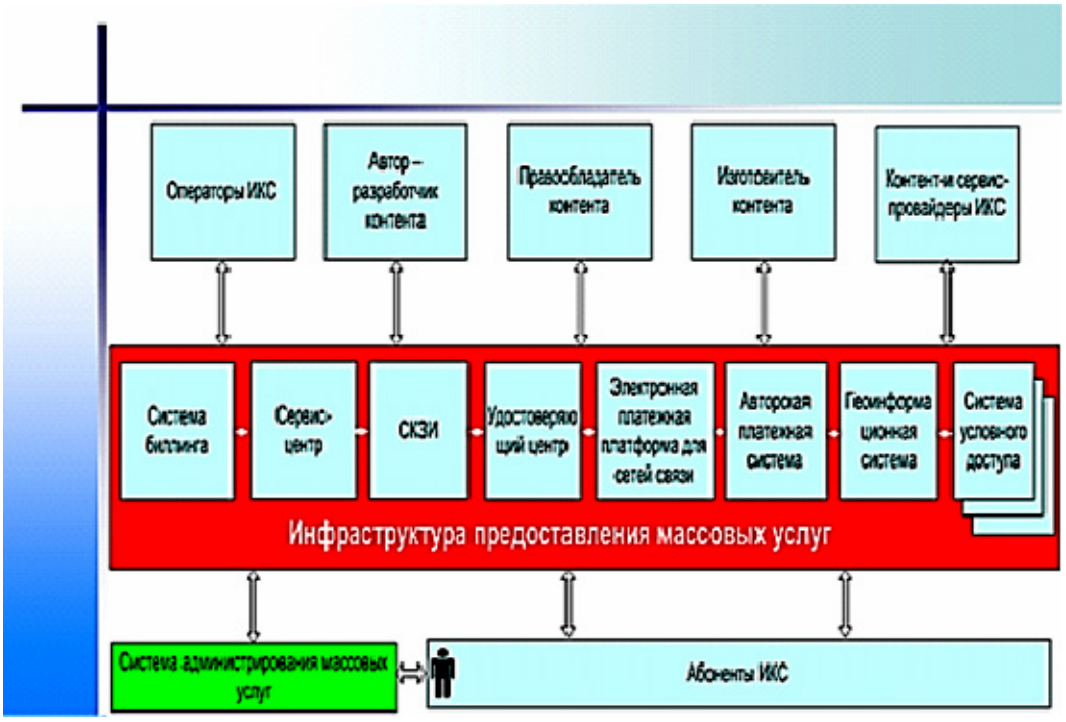



**Рис. Система администрирования предоставления гражданам ИК-услуг (САУ)**

Структурно-функциональный анализ существующей и апробированной системы администрирования услуг (САУ) показывает, что она имеет сложную структуру, элементы которой выполняют множество функций, в том числе:

- система криптографической защиты информации (СКЗИ) – программа или устройство, которые шифруют документы и генерируют электронную подпись (ЭП);

- биллинговая система – программное обеспечение, разработанное специально для операторов (провайдеров), которое позволяет считать (учитывать) и тарифицировать оказанные услуги доступа;
- авторская платежная система, защищающая авторское право правообладателя контента;
- геоинформационные технологии – системы координатно-временного и навигационного обеспечения (например, ГЛОНАСС или GPS);
- сервис-центр определяет порядок доступа к услуге и контролирует достоверность услуги, т.е. правильную работу всех ее составляющих;
- система условного доступа обеспечивает порядок взаимодействия разных поставщиков информации в случае конвергентных услуг (на рисунке для простоты не указаны).

Устойчивость предоставления ИК-услуг и функционирования САУ обеспечивается соответствующим государственным надзором. Государственный мониторинг и контроль САУ включает соблюдение критериев государственной и общегражданской безопасности, достоверности информации, реализации функций госучреждений и обязательств по их исполнению; разрешение споров сторон в максимально короткие временные, вытекающие из смысла услуги, сроки и недопущение массового нарушения прав пользователей. В основе деятельности надзорных органов должны лежать социотехнологические стандарты [Сарьян, Фролов, Назаренко, 2020] и регламенты, которые могут и должны быть выработаны в тесном взаимодействии специалистов и экспертов, компетентных в различных аспектах цифровых технологий и ИК-услуг.

Примером ИК-услуги, которая может быть рекомендована для широкомасштабного внедрения, является разработанная в ФГУП НИИР[1] индивидуализированная услуга управления спасением абонентов ИКС при возникновении чрезвычайных ситуаций (далее – ЧС) природного и техногенного происхождения. Данная услуга существенно повышает адаптационные возможности человека и повышает его безопасность.

Исследования показывают, что в современном мире мегамасштабов и сверхскоростей сенсорные реакции человека оказываются недостаточными при возникновении ЧС, что значительно увеличивает риски людских и материальных потерь. Работы, проведенные в течение 2010–2019 гг. отечественными научными организациями [Междисциплинарное сотрудничество ..., 2019; Сарьян, Назаренко, Ермаков, 2019], показали, что сенсорные способности человека можно повысить с помощью современных ИКТ, в частности «Интернета вещей» (Internet of Things), далее – IoT. Технологии IoT предполагают включенность в ИКС самостоятельно взаимодействующих между собой или с окружающей средой технических устройств и датчиков. На базе IoT становится возможным

[1] Федеральное государственное унитарное предприятие Научно-исследовательский институт Радио.

массовое предоставление услуги по индивидуализированному управлению спасением при возникновении любого вида ЧС в зоне пребывания абонента.

Сегодня во всем мире уделяется огромное внимание разработке и эксплуатации систем мониторинга за глобальными процессами, систем прогнозирования ЧС, систем оповещения населения о ЧС. Однако все принимаемые меры не могут пока повысить предсказательный потенциал существующих систем, а также обеспечить возможности эффективного спасения людей. Так, граждане, оказавшиеся в зоне ЧС (и даже предупрежденные о ЧС на основе краткосрочного прогноза), становятся беспомощными, сразу забывают все инструкции и часто оказываются жертвами ЧС. Существующие сегодня системы спасения людей (в том числе системы оповещения о ЧС) практически не управляют спасением людей во время протекания ЧС, несмотря на то что наибольшие людские потери происходят именно в это время.

Основная идея повышения сенсорных способностей личности заключается в расширении области взаимодействия человека со смарт-средой, которая в нужное время сообщит ему о предстоящих ЧС. Предупредительные сигналы человек получает на любое персональное интеллектуальное абонентское устройство, которым может быть и сотовый телефон. На таком устройстве способны отображаться разработанные модели возможных аварийных ситуаций с привязкой к определенному месту, цифровая карта местности, а также указатели индивидуального маршрута эвакуации в безопасное место – персональный навигатор в ЧС. Датчики способны считывать изменение параметров внешней среды, а система спасения – корректировать алгоритм спасения, в том числе учитывать возможные скопления людей на путях эвакуации, направлять различные команды абонентам в зависимости от их статуса, например особые распоряжения обслуживающему персоналу. Сенсорная сеть связана с оперативно-диспетчерскими службами МЧС, что повышает эффективность работы по ликвидации последствий ЧС.

Но услуга индивидуализированного управления спасением людей при возникновении ЧС бессильна, если отрезок времени между началом ЧС и его катастрофической фазой приближается к нулю, например при землетрясениях. Выход один – необходимо резко повысить предсказательный потенциал существующих систем мониторинга за такими типами ЧС. Однако используемые сегодня датчики малочувствительны к сигналам – предвестникам землетрясений, и в этой области необходимы дополнительные научные исследования.

Для достижения должной эффективности распространение системы индивидуализированного управления спасением людей при возникновении ЧС должно быть массовым и повсеместным. Последнее же невозможно представить в отсутствие прямо выраженной воли государства и соответствующих императивных нормах права.

## Заключение

В доисторическую эпоху человек сам обеспечивал свою безопасность. В эпоху государственности в этом ему стали помогать государственные институты. Безопасность граждан – одна из ключевых целей современного государства, и в цифровую эпоху оно должно для этого использовать цифровые инструменты.

Безопасность достигается функцией достоверного отражения вызовов и угроз природной и социальной среды и составления на этой основе оптимальной программы устойчивого развития. ИК-услугу по индивидуализированному спасению людей в ЧС природного и техногенного характера следует рассматривать как средство реализации государственной власти по защите гражданского общества [Российская правовая система …, 2019; Сарьян, Фролов, Назаренко, 2020], и поэтому она должна быть точкой приложения государственного регулирования. Цифровые технологии позволяют наиболее оперативным образом донести необходимые для спасения жизни и сохранения здоровья распоряжения ответственных должностных лиц непосредственно гражданам посредством мобильных средств связи. САУ может выполнить функцию контроля за соблюдением прав потребителя услуг и за качеством самой услуги. При этом важно осуществить корректную трансформацию госуслуг в ИК-услуги и массовых ИК-услуг в индивидуальные ИК-услуги. Очевидно, что повсеместное внедрение этой услуги значительно повысит безопасность граждан и государства в целом.

В заключение отметим, что отсутствие комплексного междисциплинарного подхода к разработке алгоритмов внедрения ИК-госуслуг делает проблематичной высокую скорость освоения новых технологий. Кроме того, в настоящее время возникла острая необходимость системной (социальной, политической, правовой и экономической) оценки внедрения и оптимизации государственной системы администрирования безопасности и достоверности предоставления информационных услуг гражданам.

## Список литературы

*Бутенко В.В., Назаренко А.П., Сарьян В.К.* Проблемы современного этапа и пути дальнейшего развития информационного общества // Тезисы 4-й отраслевой конференции – форум «Технологии информационного общества», 5–7 апреля 2010 г., МТУСИ. – С. 25–34.

*Вернадский В.И.* Избр. соч.: в 5 т. – Москва; Ленинград: Изд-во АН СССР, 1954. – Т. 1. – 700 с.

*Дебор Г.* Общество спектакля. – Москва: Логос, 2000. – 154 с.

Междисциплинарное сотрудничество в период с 2014 по 2019 г. по формированию массовой услуги по индивидуализированному спасению людей при возникновении ЧС природного и техногенного происхождения / Назаренко А.П., Сарьян В.К., Ермаков В.В. и др. // Труды НИИР (Научно-исследовательского института радио): сборник научных статей. – Москва, 2019. – С. 39–54.

*Назаренко А.П., Сарьян В.К.* О возрастании роли администрирования услуг КВНО на современном этапе // Труды ИПА РАН. – 2017. – Вып. 43. – С. 3–13.

Российская правовая система в условиях четвертой промышленной революции: Материалы VI Московского юридического форума XVI Международной научно-практической конференции: в 3 частях. – М.: Проспект, 2019. – Т. 1. – 507 с.

*Сарьян В.К., Левашов В.К., Назаренко А.П.* Разработка и внедрение социо-технических стандартов – эффективный инструмент оценки влияния результатов внедрения новых технологических решений на социальные параметры современного общества // Межведомственный научно-практический семинар «Стратегия развития России в контексте гуманитарно-технологической революции». – 2019. – 27.11. – С. 235–240.

*Сарьян В.К.* Определение эффективности телерадиовещания в современных условиях // Brodcasting. – 2005. – № 2. – С. 42–45.

*Сарьян В.К., Назаренко А.П., Ермаков В.В.* Повышение адаптационных возможностей человека в условиях возрастающего техногенеза и увеличения риска человеческих и материальных потерь от ЧС природного и техногенного происхождения – витальная задача (задача выживания) современной цивилизации // Большая Евразия: Развитие, безопасность, сотрудничество: ежегодник / РАН. ИНИОН. Отд. науч. сотрудничества; отв. ред. В.И. Герасимов. – Москва: ИНИОН РАН, 2019. – Вып. 2, ч. 2. – С. 730–738.

*Сарьян В.К., Фролов А.И., Назаренко А.П.* Информационные системы индивидуализированного управления как средство реализации исполнительной власти // Административно-правовые формы реализации исполнительной власти в условиях цифровизации государственного управления: сб. трудов XIII Международной научно-практической конференции, посвящ. памяти Ю.М. Козлова. – М.: МГЮА, 2020. – (в печати).

Экспресс-информация. Как живешь, Россия? XLVIII этап социологического мониторинга, ноябрь-декабрь 2018 года / под общей редакцией В.К. Левашова. [Электронное издание]. – М.: Перспектива, 2019. – URL: http://xn--h1aauh.xn--p1ai/wp-content/uploads/2019/02/%D0%AD%D0%98-%D0%9A%D0%96%D0%A0-48-%D0%BE%D0%BA%D0%BE%D0%BD%D1%87.pdf (дата обращения 08.04.2019)

*Gilbert F.S., Peterson Th.B., Schramm W.* Four Theories of Press. – Urbana: University of Illinois Press, 1956. – 168 p.

# О РОЛИ НАУЧНЫХ ИССЛЕДОВАНИЙ В РАМКАХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ОБЩЕСТВА[1]


## Зацаринный Александр Алексеевич

Доктор технических наук, заместитель директора Федерального исследовательского центра «Информатика и управление» РАН, лауреат Премии Правительства РФ в области науки и техники за 2003 г. Член Научного совета при Президиуме РАН по фундаментальным проблемам связи с глубокопогруженными объектами (Москва, Россия)



***Аннотация.*** *В статье обсуждаются следующие проблемы цифровой трансформации общества: несистемный подход к стратегическому планированию и невостребованность деятельности научных организаций. Дана краткая характеристика результатов научных исследований ФИЦ ИУ РАН по направлению «цифровизация общества». Показана роль информационных технологий в борьбе с эпидемией коронавируса и даны предложения по их развитию.*



***Ключевые слова:*** *цифровая трансформация; стратегическое планирование; научные исследования; информационные технологии; коронавирус.*

**Для цитирования:** Зацаринный А.А. О роли научных исследований в рамках цифровой трансформации общества // Социальные новации и социальные науки. – Москва: ИНИОН РАН, 2020. – № 1. – С 47–59.

URL: https://sns-journal.ru DOI: 10.31249/snsn/2020.01.04





[1] Статья подготовлена при частичной поддержке грантов РФФИ (проекты 18-29-03091-мк и 18-29-03124-мк)

## Введение

В Послании Федеральному собранию 15 января 2020 г. Президентом России В.В. Путиным поставлена задача придать национальным проектам «еще более глубокий смысл» и связать их в единую системную программу [Послание, 2020], подтверждена амбициозная задача вхождения страны в число пяти крупнейших экономик мира [Указ № 240, 2018].

Ключевым звеном успешного решения этой задачи в условиях нарастающих крупномасштабных угроз национальной безопасности России является кардинальное повышение качества решений на всех уровнях государственного управления. Именно с неэффективным управлением связана большая часть проблем в развитии экономики. Иначе трудно объяснить, почему Россия, обладающая огромными запасами мировых ресурсов (минеральных, водных, земельных), имеет незначительный вес в мировом ВВП (в 2014 г. – 2,8%, в 2018 – 1,9%), в рейтинге глобальной конкурентоспособности IMD[1] «застыла» на 45-м месте, а две самые отстающие сферы по мировым рейтингам – здравоохранение (119-е место по интегральному показателю, учитывающему 90 отдельных показателей Всемирной организации здравоохранения) и финансы (по всем показателям – ниже 100-й позиции, в том числе развитость финансов – 107-е, монетаризация – 105-е место и т.д.) [Беседы …, 2018]. Почему при таких значительных природных ресурсах государство не может обеспечить безбедную жизнь 145 млн человек, которые составляют 2% населения планеты?!

Новые глобальные вызовы 2020 г., обусловленные всемирной пандемией, вызванной широким распространением коронавируса, а также резким падением мировых цен на нефть, указывают на значимость и актуальность кардинального повышения эффективности управления. Важно в связи с этим, что новый Председатель Правительства России М.В. Мишустин в своем программном выступлении в Государственной думе РФ как одну из целей правительства обозначил повышение качества управления («…важнейший вопрос – это новое качество управления») и акцентировал внимание на стимулировании цифровизации реального сектора экономики в рамках национального проекта «Цифровая экономика» [Мишустин …, 2020].

Российские ученые могут предоставить научно обоснованные направления улучшения качества управления и формирования эффективных ответов на вызовы современности.

[1] Швейцарская бизнес-школа.

## Системный подход к стратегическому планированию в рамках цифровой трансформации

Сегодня в экспертном сообществе справедливо полагают, что курс на цифровую экономику – последний шанс не отстать от мирового развития [Информационное пространство ..., 2018]. Цифровая трансформация общества неизбежна. Десятки миллионов цифровых устройств (компьютеры, смартфоны, коммуникаторы, планшеты и др.) стали доступны не только организациям, но и каждому физическому лицу. Обосновано, что в Стратегии научно-технологического развития России в качестве первого приоритета определены именно цифровые технологии [Указ № 642, 2016]. Внедрение этих технологий должно позволить в ближайшие 10–15 лет получить новые научные и научно-технические результаты, необходимые для инновационного развития страны [Программа, 2017]. Вместе с тем все более острой становится проблема системности внедрения и применения огромного множества цифровых устройств. Здесь и совместимость, и унификация, и защита персональных данных, и, наконец, грамотность и культура использования, и многое другое.

Однако в настоящее время становится все более очевидным, что недавние ожидания не подкрепляются реальными результатами. Так, на заседании Государственной думы РФ 8 июля 2019 г., посвященном состоянию цифровой экономики, ни в одном из докладов руководителей ответственных министерств (Минэкономразвития, Минкомсвязи), Банка России, Сбербанка России не просматривался системный подход к развитию цифровой экономики, не отмечены роль и место научных организаций в Программе цифровой экономики, не показана взаимосвязь с работами по цифровизации и внедрению цифровых платформ в рамках других нацпроектов. Более того, спикер Государственной думы РФ В. Володин обратил внимание на срыв плана по разработке и представлению нормативных документов [Стенограмма, 2019].

Представляется, что одна из ключевых проблем цифровой трансформации российского общества – это отсутствие системного подхода к стратегическому целеполаганию при планировании работ. Достаточно упомянуть, что пять базовых направлений в Программе цифровой экономики выглядят обособленно и несвязанно. В дополнение к этим направлениям обязательно должно быть сформировано еще одно, под условным названием «Система “Цифровая экономика” (СЦЭ), в рамках которого должны быть определены основные организационные, методологические и системотехнические решения [Зацаринный, Ионенков, Козлов, 2010; Информационное пространство …, 2018; Зацаринный, 2019].

Данное системное направление призвано стать задающим вектором для всех остальных направлений и позволило бы конкретизировать деятельность по подготовке комплекса нормативных документов, по обучению и подготовке необходимых кадров, по обоснованию профиля необходимых информационных технологий, по созданию инфраструктуры (прежде всего, в регионах) и, наконец, по обеспечению информационной безопасности.

Пока ничего похожего на системность в комплексе выполняемых работ не наблюдается. Например, в принятой в конце 2018 г. новой Национальной программе «Цифровая экономика» (взамен ранее действовавшей) не приводится перечень сквозных технологий, но включены дорожные карты по их развитию.

Еще один аспект: с принятием курса на цифровую экономику наметилась тенденция смешения понятий «цифровая экономика» и «экономика». Однако это вопрос принципиальный: цифровая экономика – это не экономика! Цифровой экономикой можно охватить все то, что поддается формализации, т.е. превращению в цифровые логические схемы. А жизнь сама найдет возможность вписать это «нечто» в систему производства, распределения, обмена или потребления [Информационное пространство …, 2018].

Другими словами, цифровая экономика – это некая технологическая надстройка, которая может обеспечить повышение уровня управляемости реальной экономикой как совокупностью конкретных активов в различных областях (транспорт, связь, сельское хозяйство, промышленное производство, добывающие отрасли, сфера услуг и торговли и др.). И поэтому задачи цифровой экономики и задачи развития различных отраслей реальной экономики должны быть системно взаимоувязаны. В этом суть цифровой трансформации общества в направлении его экономического развития. Только при реализации такого системного подхода может быть обеспечена эффективность управленческих решений в цифровой экономике на всех уровнях, что приведет к минимизации влияния человеческого фактора и сокращению числа уровней в иерархии системы управления.

Успешная реализация программы цифровой экономики будет иметь нулевой эффект, если не будут предприняты кардинальные шаги по развитию конкретных отраслей экономики. И, наоборот, развитие реальной экономики не позволит получить ощутимые результаты без внедрения самых современных цифровых технологий.

Еще одной важной проблемой цифровой трансформации России является кризис института руководителей, способных принимать эффективные и компетентные решения в условиях современных вызовов [Информационное пространство ..., 2018; Зацаринный, 2019; Зацаринный, 2020; Кондратьев, 2016].

Назначение новым председателем Правительства России человека с опытом практической работы в сфере информационных систем, а также обновление состава Правительства РФ вселяют некоторые надежды на перемены к лучшему в области эффективности процессов цифровой трансформации. Так, 1 февраля 2020 г. новый премьер поручил Минкомсвязи РФ разработать требования к кандидатам на должность заместителя руководителя федерального органа, ответственного за цифровую трансформацию общества. Можно предположить, что эта инициатива будет

иметь далеко идущие последствия в части решения организационных проблем и повышения ответственности руководителей на различных уровнях за цифровую трансформацию. Более того, на основе создаваемого контура таких заместителей руководителей ведомств было бы логичным создать под руководством председателя Правительства РФ Межведомственный совет по вопросам информационного пространства России.

В настоящее время в связи с пандемией коронавируса актуальность обеспечения межведомственного информационного взаимодействия резко возросла.

## Роль научных институтов в развитии цифровых технологий

К одному из «мегатрендов» развития информационных технологий цифровой экономики сегодня по праву относится искусственный интеллект. Об этом свидетельствует ряд фактов. Например, по прогнозам известной компании Accenture (США), искусственный интеллект (ИИ) становится важнейшим фактором производства, который способствует продвижению инноваций в экономике и приводит к созданию «виртуальной рабочей силы». Прогнозируется, что наибольшие темпы роста за счет ИИ ожидаются в американской экономике (4,6%), а также в Финляндии (4,1%) и Великобритании (3,9%). Внедрение технологий ИИ может принести мировой экономике 15,7 трлн долл. [Accenture].

В США предусмотрен комплекс мероприятий по интенсификации работ в области ИИ на основе указа Президента от 11.02.2019 «О сохранении американского лидерства в области искусственного интеллекта» [Указ Президента США, 2019].

В 2019 г. по поручению Президента РФ ПАО Сбербанк РФ разработал Национальную стратегию развития искусственного интеллекта на период до 2030 г. (утверждена Указом Президента РФ от 10.10.2019 г. № 490) (далее – Стратегия). Однако при подготовке Стратегии не были в полной мере учтены замечания ведущих российских ученых в области ИИ. Так, в документе не нашел отражения тот факт, что в России уже более 30 лет существуют профессиональное сообщество и научные школы в области ИИ, вполне достойно представленные как на европейском, так и на мировом уровнях. Академические институты в результате многолетних исследований накопили солидные научные заделы в этой области, подготовлено молодое поколение специалистов в области ИИ. Кроме того, в Стратегии не упомянуты собственно задачи управления (а не принятия управленческих решений), неверно трактуется предназначение систем ИИ (п. 21) [Указ № 490, 2019]. И, к сожалению, до настоящего времени по этой Программе не определен ответственный федеральный орган власти.

Россия уже не входит в число ведущих научных стран мира. За последние десять лет (2008–2019) в среднем каждая четвертая научная публикация (25%) принадлежит американским ученым, пятая – китайским (21%), а российским – только одна из ста (1%) [Наука, 2019]. Вместе с тем ве-

дущие научные организации России обладают значительным научным заделом в части методов и технологий ИИ.

Примером может служить коллектив Федерального исследовательского центра «Информатика и управление» РАН (ФИЦ ИУ РАН). В 2019 г. ФИЦ ИУ РАН разработал проект научно-технической программы «Искусственный интеллект как драйвер цифровой трансформации экономики России», а также проект комплексной программы его развития. Оба документа были одобрены Советом по приоритетным направлениям Стратегии научно-технологического развития России.

Для повышения эффективности проведения экспериментальных исследований цифровой трансформации в ФИЦ ИУ РАН создана специальная цифровая платформа, представляющая собой совокупность центра компетенций, высокопроизводительного вычислительного комплекса (ГВВК) и научных сервисов (аналитических, образовательных, библиотечных, вычислительных и др.), которые могут предоставлять услуги представителям различных сфер деятельности (образования, науки, бизнеса, государственных структур) [Зацаринный, 2018; О некоторых подходах …, 2017].

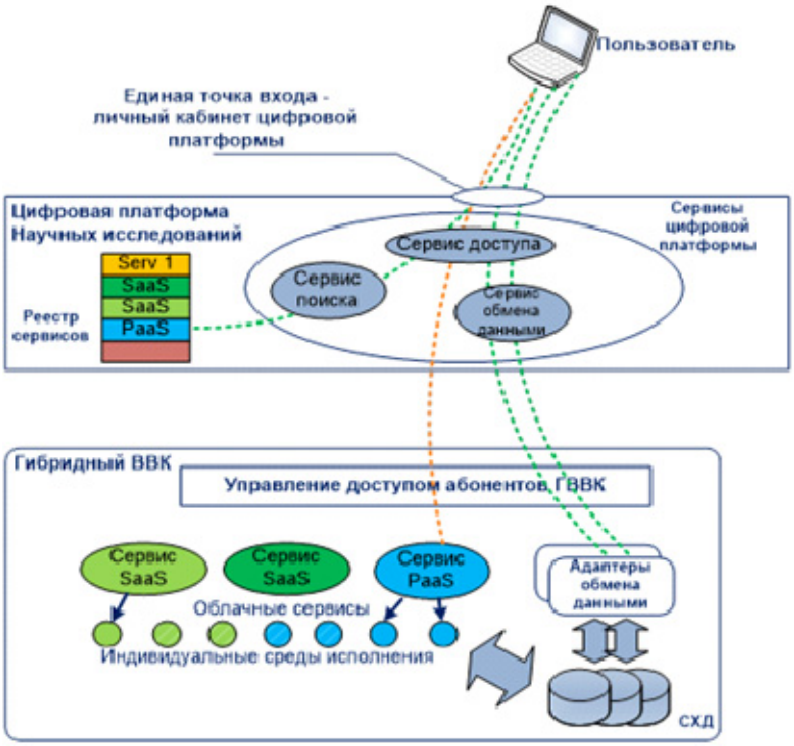



**Рис. Высокопроизводительный вычислительный комплекс (ГВВК) ФИЦ ИУ РАН**

На базе ГВВК создан и зарегистрирован центр коллективного пользования (ЦКП) «Информатика» [Положение о ЦКП, 2019], который предоставляет вычислительные ресурсы, включая: облачные сервисы SaaS для проведения расчетов на базовом ПО; облачные сервисы PaaS для развертывания всех видов программных комплексов (frameworks) в индивидуальной виртуальной среде docker; онлайн-доступ пользователей к инструментальным средствам ГВВК; интерактивную

и пакетную обработку вычислительных заданий; личный кабинет пользователя вычислительных сервисов, а также единую точку входа и вспомогательные сервисы цифровой платформы (рис.).

Под руководством д-ра физ-мат. наук К.К. Абгарян в ФИЦ ИУ РАН выполняются исследования по многомасштабному моделированию для синтеза материалов с заданными свойствами, направленные на разработку алгоритмов машинного обучения и методов управления большими данными для решения задач квантово-механического моделирования [Абгарян, 2017; Зацаринный, Абгарян, 2019].

Исследования проблемных вопросов управления робототехническими устройствами в ФИЦ ИУ РАН направлены на создание интеллектуальных роботов и изыскание новых алгоритмов управления робототехническими устройствами. Уже разработан ряд методов символьной регрессии (сетевого оператора, вариационного генетического и аналитического программирования, бинарного вариационного генетического программирования), а также подход для оптимального решения на основе принципа малых вариаций базисного решения [Diveev, Shmalko, Sofronova, 2018; Diveev, Shmalko, Zakharov, 2017].

В ФИЦ ИУ РАН проводятся исследования в области информационной безопасности с учетом новых вызовов и угроз, обусловленных процессами цифровой трансформации общества. Ученые пришли к выводу, что использование известных уязвимостей в атаках будет возрастать с учетом расширения атакуемой информационной поверхности предприятий. Кроме того, поскольку все больше устройств производятся без учета правил безопасности и отраслевых стандартов, прогнозируется рост числа уязвимостей в области Интернета вещей (IoT) [Изменения парадигмы, 2018].

Новые угрозы и риски создает широкое применение облачных технологий, так как в них «размывается» ключевое понятие в парадигме защиты – понятие контура системы. Поэтому теперь центр тяжести должен смещаться от существующего ограничительно-запретительного подхода к новому, основанному на мониторинге действий пользователей, состава и состояния программно-технических средств с использованием технологий ИИ [Гаврилов, Зацаринный, 2016; Зацаринный, Гаврилов, 2017].

На первый план в условиях цифровой трансформации общества выходит обеспечение целостности и доступности информации, корректность реализации алгоритмов функционирования в прикладном программном обеспечении, непротиворечивость и полнота этих алгоритмов. В связи с этим требуется кардинальное изменение парадигмы защиты информации. В ее основу должны быть положены такие понятия, как комплексность, функциональность и системность [Зацаринный, Гаврилов, 2017].

Важным научно-практическим направлением работы ФИЦ ИУ РАН являются исследования, разработка, гармонизация международных стандартов ИСО / МЭК и подготовка проектов новых стандартов в области информационной безопасности и защиты информационных технологий. Такая работа выполняется по заказу Росстандарта с целью поддержания национального фонда стандартов в области информационной безопасности на современном научно-техническом уровне.

Под руководством д-ра физ.-мат. наук проф. В.А. Серебрякова в ФИЦ ИУ РАН исследуются вопросы формирования пространства научных знаний (ПНЗ). Ключевым в этом направлении является понятие *цифровой семантической открытой библиотеки*, которая обеспечивает поддержку использования различных типов ресурсов, включая медийные объекты (текст, аудио- и видеофайлы или их комбинации), и связей между ними, предоставляет возможность связывания своих данных с данными из открытых источников. Создан и зарегистрирован программный комплекс «Цифровая семантическая открытая библиотека LibMeta» [Атаева, Серебряков, 2018].

Другим важным результатом является разработка *модели электронной бухгалтерской книги для описания цифровой экономики* на региональном уровне, в основу которой положен *тангл* как модернизированная версия блокчейна. С помощью танглов, связанных с отдельными субъектами экономической деятельности, можно контролировать выполнение проектов, в том числе с использованием государственных инвестиций [Грушо, Зацаринный, Тимонина, 2019, Grusho, Zatsarinny, Timonina, 2019].

Комплексные исследования по оценке влияния процессов цифровизации на качество жизни человека, проводимые в ФИЦ ИУ РАН (под руководиством д-ра тех. наук проф. К.К. Колина), показали, что новые информационно-коммуникационные технологии (ИКТ) обеспечивают людям оперативный доступ к необходимой им социально значимой информации, позволяют сократить время для решения многих производственных и бытовых проблем, а также повышают уровень личной безопасности. Растет уровень комфортности среды обитания человека как в городах, так и в сельской местности. Характерным примером может служить быстрое распространение навигационных космических информационных систем типа ГЛОНАСС и GPS в разных странах мира. Их использование позволило упорядочить движение автотранспорта во многих городах, обеспечить наблюдение за транспортными перевозками грузов и повысить их безопасность [Информационное пространство …, 2018].

Полученные в ФИЦ ИУ РАН результаты в области методологии измерения и комплексного индикаторного оценивания качества жизни населения свидетельствуют, что цифровая трансформация влечет за собой не только позитивные, но и негативные последствия. В частности, ожидаются существенные изменения в структуре занятости населения, что может привести к усилению социального неравенства, росту безработицы и повышению уровня социальной напряженности.

Разработанная в институте *методология количественной оценки уровня социальной стабильности общества* может быть использована для мониторинга ситуации в различных странах или отдельных регионах [Колин, 2010; Колин, 2018; Зацаринный, Колин, 2018].

## Информационные технологии в борьбе с эпидемией коронавируса

Эпидемия коронавируса – новый и неожиданный глобальный вызов всему человечеству. Абстрагируясь от дискуссии о природе коронавируса, отметим, что пострадать может каждый, независимо от социального положения, интеллекта и уровня обеспеченности.

Очевидно, что ИКТ должны сыграть значительную роль в комплексе мероприятий по борьбе с пандемией, в том числе по следующим направлениям.

Обеспечение *режима «удаленной работы».* Данный формат работы пока не имеет официального статуса, и даже не существует единого понятия, несмотря на достаточно распространенную практику. Минтруд России только планирует внести соответствующие поправки в трудовое законодательство (Трудовой кодекс дополнят статьей «Временная удаленная работа»), которые позволят совмещать работу из дома и офиса.

Кроме того, удаленный режим работы требует соответствующей информационной, технической и телекоммуникационной поддержки. Речь идет о технических регламентах информационного взаимодействия с офисом, информационного взаимодействия сотрудников между собой, проведения технических совещаний в режиме онлайн, обеспечения оперативного оповещения и информирования сотрудников, технической и технологической оснащенности домашних рабочих мест сотрудников и многое другое. В настоящее время существует много решений для большинства из этих задач, в том числе появилось множество корпоративных мессенджеров, сервисов аудио- и видеосвязи, благодаря которым рабочий процесс из дома мало отличается от офисного. Более того, многие сотрудники уже работают в удаленном (дистанционном) режиме. Однако сейчас происходит массовый переход на удаленную работу, и необходимо все эти возможности регламентировать на государственном уровне, определить в положении о дистанционной работе и в договоре с работодателем. При этом очень важно учесть и требования по защите информации.

*«Дистанционное обучение».* В последнее время на такую форму перешли практически все вузы. В данной области существует как набор общих технологий, так и специфические для каждого вуза, что определяет необходимость изучения лучших практик. Отдельной проработки требуют вопросы информационной поддержки удаленного обучения учащихся школ. Например, в Китае более 200 млн детей начали весенний семестр в онлайн-классах, организованы прямые трансляции уроков, а Министерство образования Китая представило «национальный облачный интернет-класс», который способен принимать до 50 млн учеников начальной и средней школы одновременно [Полякова, 2020; Как для борьбы …, 2020].

Обеспечение так называемого *бытового режима карантина,* когда люди массово обязаны проводить время в квартирах, на дачах и т.д. Следует предложить им социально направленные онлайн-передачи, фильмы, культурные программы, онлайн-концерты и т.д. Главное при этом – сохранять управляемость процессом.

В условиях эпидемии коронавируса *социальные сети* одновременно являются и благом, и злом. В первом качестве предоставляют возможность получать оперативную информацию, общаться и обмениваться мнениями. Во втором – содействуют распространению дезинформации и фейковых новостей. В кризисных условиях ложная информация особенно негативно влияет на настроения в обществе, поэтому необходимо усилить контроль за распространением информации о ходе пандемии со стороны соответствующих органов.

Развитие и совершенствование *технологий мониторинга, распознавания и анализа данных* о перемещениях физических лиц и транспортных средств. Так, в Китае был налажен весьма эффективный контроль перемещения людей с помощью систем видеонаблюдения, учитывающих их походку и нахождение в масках. В Гуанчжоу на входе в учреждение или жилое помещение помимо температурного контроля обязательно проверялся статус в двух WeChat-приложениях. В первом генерировался (с обновлением каждые семь суток) QR-код, который хранил историю медицинских посещений, если такие были. Во втором приложении содержалась информация от сотового провайдера за последние 14 дней о «прохождении» СИМ-карты внутри Китая и в других странах. На основе проверок по этим двум приложениям учреждение принимало решение о допуске [Как для борьбы …, 2020].

Использование *беспилотных транспортных средств*, управляемых роботами, для доставки продуктов, медикаментов и других необходимых вещей с целью исключения или минимизации контактов между людьми.

*Защита информации*. Эксперты Group-IB прогнозируют рост числа кибератак на компьютеры, оборудование и незащищенные домашние сети сотрудников компаний, которые перешли на удаленный режим работы. В группе риска, прежде всего, – персонал финансовых учреждений, телеком-операторов, IT-компаний, туристических фирм (центры возврата денежных средств авиалиний, отелей и т.д.), а также люди пожилого возраста (доставка товаров на дом, предложения лекарств и тестов на COVID-19 и другое). Целью кибератак является кража денег или персональных данных. В связи с этим необходима разработка и реализация комплекса организационно-технических мер, включая процедуры авторизации (желательно многофакторной) и аутентификации, закрытия передаваемой информации, ведения журналов удаленных действий пользователей и другие меры.

Резкое *сокращение оборота наличных денег* (как возможных переносчиков вируса) вплоть до их полного исключения, по крайней мере в крупных городах. Реализация данной меры потребует соответствующей информационной поддержки. Хотя в Китае масштабный переход на использование безналичных расчетов был организован в кратчайшие сроки посредством использования национальных платежных систем WeChat pay и Alipay [Как для борьбы …, 2020].

Для осуществления предлагаемых направлений необходимо определить ответственных заказчиков (при ведущей роли Министерства цифрового развития, связи и коммуникаций РФ), провести корректировку национальных проектов, прежде всего «Цифровая экономика» и «Наука», привлечь к подготовке профильные научные организации.

## Заключение

1. Задачи цифровой экономики и развития различных отраслей реальной экономики должны быть системно взаимоувязаны. Цифровая экономика как высокоинтеллектуальная инфраструктурная технологическая надстройка должна обеспечить повышение уровня управляемости реальной экономикой как совокупностью конкретных активов в различных областях (промышленность, транспорт, добывающие отрасли, медицина и др.). В этом суть цифровой трансформации.

2. Важнейшие цели, поставленные руководством страны по цифровой трансформации общества, могут быть достигнуты только на основе усиления системного подхода при стратегическом планировании и целеполагании, активного привлечения к работам в рамках цифровой экономики научных организаций страны, а также преодоления кризиса института руководителей на новом организационно-методическом уровне. Современный руководитель помимо базовых знаний в конкретной предметной области должен обладать необходимым уровнем знаний в области информационных технологий. Это – неизбежный вызов цифровой трансформации общества на всех уровнях его жизнедеятельности.

3. Как никогда ранее актуальной становится синергетика теории и практики – результатов фундаментальных исследований и положительного опыта создания информационных систем. Для этого необходимо объединить науку (фундаментальную, прикладную, военную), технологии и промышленное производство.

4. ФИЦ ИУ РАН обладает большим научным потенциалом в области компьютерных наук (около 500 дипломированных сотрудников), а также уникальными результатами исследований в области информатики, которые находят применение при разработке, внедрении, модернизации и сопровождении информационно-телекоммуникационных систем в интересах органов государственной власти на различных уровнях.

5. Новые глобальные вызовы, связанные с пандемией коронавируса, требуют принятия срочных мер по организации использования и соответствующей адаптации ИКТ, включая корректи-

ровку национальных проектов, прежде всего «Цифровая экономика» и «Наука», и привлечения к этой работе профильных научных организаций.

## Список литературы

*Абгарян К.К.* Многомасштабное моделирование в задачах структурного материаловедения. – М.: МАКС Пресс, 2017. – 284 с.

*Атаева О.М., Серебряков В.А.* Онтология цифровой семантической библиотеки LibMeta // Информатика и ее применение. – 2018. – Т. 12, вып. 1. – С. 2–10.

Беседы об экономике / Вольное экономическое общество; под редакцией д-ра э.н. С.Д. Бодрунова. – М: ИНИР им. С.Ю. Витте, 2018. – Т. 8. – 385 с.

*Гаврилов В.Е., Зацаринный А.А.* Некоторые системотехнические и нормативно-методические вопросы обеспечения защиты информации в АИС на основе облачных технологий с использованием технологий искусственного интеллекта // Системы и средства информатики. – М.: ТОРУС ПРЕСС, 2016. – Т. 26, № 4. – С. 40–52.

*Грушо А.А., Зацаринный А.А., Тимонина Е.Е.* Угрозы электронной бухгалтерской книге, построенной на базе Tangles // Методы и технические средства обеспечения безопасности информации. – 2019. – № 28. – С. 70–71.

*Зацаринный А.А. Гаврилов В.Е.* Кибербезопасность и право // Транспортная безопасность и технологии. – 2017. – № 4 (51). – С. 90–93.

*Зацаринный А.А.* Ключевые проблемы цифровой трансформации общества // Сборник материалов XX Международной конференции «Информатика: проблемы, методы, технологии» (IPMT-2020) / под ред. Д.Н. Борисова. – М.: Издательство «Научно-исследовательские публикации» (ООО «Вэлборн»), 2020. – (в печати).

*Зацаринный А.А.* Методологические аспекты стратегического целеполагания в условиях цифровой трансформации России: доклад // Материалы Двенадцатой международной конференции «Управление развитием крупномасштабных систем MLSD», 1–3 октября 2019, Москва. – М., 2019. – С. 126–132.

*Зацаринный А.А.* Цифровая платформа для научных исследований // Математическое моделирование и информационные технологии в инженерных и бизнес-приложениях: сборник материалов междунар. науч. конф. (3–6 сентября 2018 г.) / под ред. М.Г. Матвеева, Д.Н. Борисова; Воронежский государственный университет. – Воронеж: Издательский дом ВГУ, 2018. – С. 104–113.

*Зацаринный А.А., Абгарян К.К.* Факторы, определяющие актуальность создания исследовательской инфраструктуры для синтеза новых материалов в рамках реализации приоритетов научно-технологического развития России // Материалы I международной конференции «Математическое моделирование в материаловедении электронных компонентов. ММММЭК-2019». – М.: МАКС Пресс, 2019. – С. 8–11.

*Зацаринный А.А., Ионенков Ю.С., Козлов С.В.* Некоторые вопросы проектирования информационно-телекоммуникационных систем. – М.: ИПИ РАН, 2010. – 218 с.

*Зацаринный А.А., Колин К.К.* Технология «Измерение и оценка уровня социальной стабильности в обществе» // Стратегическое целеполагание в ситуационных центрах развития. – М.: Когито-Центр, 2018. – С. 295–300.

Изменения парадигмы: прогнозы по информационной безопасности 2018 // Trend Micro Incorporated. – 2018. – URL: https://www.securitylab.ru/news/490280.php (дата обращения 10.03.2020.)

Информационное пространство цифровой экономики: концептуальные основы и проблемы формирования / Зацаринный А.А., Киселев Э.В., Козлов С.В., Колин К.К. – М.: ФИЦ ИУ РАН, 2018. – 236 с.

Как для борьбы с коронавирусом в Китае используют высокие технологии // BIGPicture. – 2020. – URL: https://bigpicture.ru/?p=1282419 (дата обращения 10.03.2020.)

*Колин К.К.* Качество жизни в информационном обществе // Человек и труд. – 2010. – № 1. – С. 39–43.

*Колин К.К.* Качество жизни: новая методология измерения // Стратегические приоритеты. – 2018. – № 4. – С. 78–85.

*Кондратьев Э.В.* Развитие управленческого персонала предприятия: системно-институциональный подход. – М.: Академический проект, 2016. – 352 с.

Мишустин представил Госдуме свою программу // РБК. – 2020. – 16.01. – URL: https://www.rbc.ru/politics/16/01/2020/5e2046379a794749e1cceb81 (дата обращения 10.03.2020.)

Наука. Технологии. Инновации: 2019: краткий статистический сборник / Н.В. Городникова, Л.М. Гохберг, К.А. Дитковский и др.; Нац. исслед. ун-т «Высшая школа экономики». – М.: НИУ ВШЭ, 2019. – 84 с. – URL: https://www.hse.ru/data/2018/12/11/1144786145/niio2019.pdf. (дата обращения 10.03.2020.)

О некоторых подходах к представлению научных исследований как облачного сервиса / Волович К.И., Зацаринный А.А., Кондрашев В.А., Шабанов А.П. // Системы и средства информатики. – М.: ТОРУС ПРЕСС, 2017. – Т. 27, № 1. – С. 73–84.

Паспорт Национального проекта «Наука» // Официальный сайт Правительства РФ. – 2019. – URL: http://government.ru/info/35565/ (дата обращения 10.03.2020)

Положение о ЦКП «Информатика» // Федеральный исследовательский центр «Информатика и управление» РАН. – 2019. – URL: http://www.frccsc.ru/sites/default/files/docs/ckp/%D0%9F%D0%BE%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%B8%D0%B5%20%D0%BE%20%D0%A6%D0%9A%D0%9F.pdf?343 (дата обращения 10.03.2020)

*Полякова А.* Как Китай использует технологии для борьбы с коронавирусом // rb.ru. – 2020. – 03.03. – Режим доступа: https://rb.ru/story/fighting-coronavirus-with-technology/ (дата обращения 10.03.2020.)

Послание Президента РФ Федеральному собранию 2020 // Официальный сайт Президента РФ. – 2020. – URL: http://kremlin.ru/events/president/news/62582/ (дата обращения 15.03.2020.)

Программа «Цифровая экономика Российской Федерации» // Официальный сайт Правительства РФ. – 2017. – URL: http://government.ru/docs/28653/ (дата обращения 10.03.2020)

Рейтинг World Research Institutions Ranking (WRIR) // Официальный сайт Европейской научно-промышленной палаты. – 2018. – URL: http://eurochambres.org/wrir/wrir-2018/informatsionnye-tekhnologii/ (дата обращения 10.03.2020.)

Стенограмма парламентских слушаний Комитета Государственной Думы по экономической политике, промышленности, инновационному развитию и предпринимательству на тему: «Вопросы развития цифровой экономики». – М., 2019. – 08.07. – 127 с.

Стратегическое целеполагание в ситуационных центрах развития / под ред. В.Е. Лепского и А.Н. Райкова. – М.: Когито-Центр, 2018. – 320 с.

Указ Президента Российской Федерации от 01.12.2016 № 642 «О Стратегии научно-технологического развития Российской Федерации» // Официальный сайт Президента РФ. – 2016. – URL: http://kremlin.ru/acts/bank/41449 (дата обращения 10.03.2020)

Указ Президента Российской Федерации от 10.102019 № 490 «О развитии искусственного интеллекта в Российской Федерации» // Консультант плюс. – URL: http://consultant.ru/ (дата обращения 10.03.2020.)

Указ Президента РФ от 07.05.2018 № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» // Консультант плюс. – URL: http://www.consultant.ru/document/cons_doc_LAW_297432/ (дата обращения 10.03.2020.)

Указ Президента США от 11.02.2019 «О сохранении американского лидерства в области искусственного интеллекта» // Официальный сайт Белого Дома США. – URL: https://www.whitehouse.gov/presidential-actions/executive-order-maintaining-american-leadership-artificial-intelligence (дата обращения 10.03.2020.)

Accenture: Искусственный интеллект ускорит ежегодные темпы экономического роста к 2035 году // Inc. – URL: https://incrussia.ru/news/accenture-iskusstvennyy-intellekt-uskorit-ezhegodnye-tempy-ekonomicheskogo-rosta-k-2035-godu/ (дата обращения 10.03.2020.)

*Diveev A.I., Shmalko E.Yu., Sofronova E.A.* Problem of Optimal Area Monitoring by Group of Robots and its Solution by Evolutionary Algorithm // Proceedings the 13 th IEEE Conference on Industrial Electronic and Applications. ICIEA 2018. – 31 May – 02 June 2018. – Wuhan, Chine, 2018. – P. 141–146.

*Diveev A.I., Shmalko E.Yu., Zakharov D.N.* Acceleration of the multilayer network operator method using MPI for mobile robot team control synthesis// XIIth International Symposium «Intelligent Systems», INTELS'16, 5–7 October 2016. – Moscow: Procedia Computer Science, 2017. – N 103. – P. 88–93.

*Grusho A., Zatsarinny A., Timonina E.* A System Approach to Information Security in Distributed Ledgers on the Situational Centers Platform // International Journal of Open Information Technologies. – 2019. – Vol. 7. N 12. – P. 46–50.

# ТОЧКА ЗРЕНИЯ

## МЕЖДУНАРОДНОЕ РЕГУЛИРОВАНИЕ КИБЕРПРОСТРАНСТВА: ВОЗМОЖНО ЛИ ЭФФЕКТИВНОЕ ВЗАИМОПОНИМАНИЕ?

**Коровкин Владимир Владиславович**

Руководитель направления «Инновации и цифровые технологии», профессор бизнес-практики Московской школы управления СКОЛКОВО (Москва, Россия.

***Аннотация.*** *Ключевым вызовом для эффективного правового регулирования киберпространства является его архитектурная трансграничность. Цель данной статьи состоит в анализе противоречий между позициями основных стран – участниц дискуссий по вопросам международного регулирования киберпространства. В связи с малой вероятностью достижения в обозримом будущем широкого международного консенсуса в области киберправа прогнозируется регионализация киберпространства, с созданием союзов, основанных на взаимном доверии участников и единстве взглядов на принципы киберрегулирования.*

***Ключевые слова:*** *цифровизация; киберпространство; киберрегулирование; международная кибербезопасность.*

**Для цитирования:** Коровкин В.В. Международное регулирование киберпространства: возможно ли эффективное взаимопонимание? // Социальные новации и социальные науки. – Москва: ИНИОН РАН, 2020. – № 1. – С. 60–76.

URL: https://sns-journal.ru/ DOI: 10.31249/snsn/2020.01.05

## Введение

Понятие «киберпространство» появилось в научно-фантастической литературе в начале 1980-х годов [Benedikt, 1991 a, p. 1], но уже через несколько лет было введено в научный оборот для описания растущего феномена глобального обмена информацией с помощью компьютерных устройств. В 1990 г. была проведена первая международная научная конференция по киберпространству (в Университете Техаса, Остин), год спустя вышел сборник статей под редакцией архитектора-урбаниста и философа Майкла Бенедикта. В своей программной статье в этом сборнике М. Бенедикт дал такую характеристику этому феномену:

> «Киберпространство – это глобально связанная многомерная искусственная или "виртуальная" реальность, поддерживаемая компьютерами, доступная через компьютеры и создаваемая компьютерами… Киберпространство имеет [свою] географию, физику, природу и [свое] *верховенство человеческого закона»* (выделено мной. – *В. К.*) [Benedikt, 1991 b, p. 122–123].

Примечательно, что вопрос о праве и законе в киберпространстве возник на заре осознания нового феномена. Тридцать лет спустя этот вопрос остается в значительной степени нерешенным, несмотря на многочисленные усилия на национальном и международном уровнях. Ключевым вызовом для эффективного правового регулирования киберпространства является его принципиальная глобальность, трансграничность. При этом имеет место парадокс: с одной стороны, информационные сети, составляющие основу киберпространства, представляются своего рода глобальным общественным благом (подобным мировому океану или атмосфере). С другой стороны, они функционируют и развиваются благодаря усилиями преимущественно частных акторов, которые сосредоточены в весьма небольшом количестве юрисдикций [Коровкин, 2019, с. 152]. Этот парадокс делает относительно малоэффективным национальное регулирование киберпространства. Кроме того, подходы нескольких отдельных суверенов к киберправу определяют де-факто международную правовую практику.

Данная ситуация вызывала и вызывает озабоченность ряда стран. Наиболее определенно высказывались Россия и Китай, которые на протяжении последних двух десятилетий предлагали идею создания международного регулирования киберпространства в виде обязывающей конвенции. Эта идея не находила понимания в США и странах Европейского союза. Ситуация в значительной степени зашла в тупик [Kerttunen, Tikk, 2018], особенно после осложнения общей геополитической ситуации в середине 2010-х годов. В 2017 г. межправительственная группа экспертов под эгидой ООН не смогла выпустить консенсусный документ по итогам заседания, причем пред-

ставители России и США обменялись весьма резкими заявлениями, фактически отказывая друг другу в статусе добронамеренных (bona fide) акторов. Непосредственным поводом для столкновения стала дискуссия вокруг принципиального подхода к кибервойне[1]. Однако круг разногласий между странами гораздо шире.

Характерные цитаты из встречных официальных заявлений показывают глубину взаимного недоверия. По мнению российского спецпредставителя, достижению консенсуса мешают: «…определенные страны, которые стремятся навязать всему миру свои правила игры в информационном пространстве… Основываясь на своих технологических достижениях, они пытаются обеспечить “право сильного” в информационном пространстве» [МИД РФ, 2017]. В свою очередь, спецпредставитель США заявил: «Я прихожу к печальному заключению, что те, кто не желает подтвердить применимость международных правовых норм и принципов [к кибервойне] считают, что их государства свободны действовать… через киберпространство для достижения своих политических целей без каких-либо пределов или ограничений для их действий» [Department of State, 2017].

Создание международного законодательства является во многих отношениях более сложным процессом, чем национальное законотворчество. Международный закон может быть установлен исключительно консенсусом всех участвующих сторон; страны имеют возможность не присоединяться к нему, причем решение о присоединении (ратификация уполномоченными национальными органами власти, обычно парламентами) практически всегда становится результатом сложного внутреннего политического процесса. Акторы международного пространства осознают себя как находящихся в сложной конкурентной ситуации с неравными стартовыми позициями и по этой причине: 1) ищут способы ее усиления и 2) предполагают, что другие участники процесса действуют аналогичным образом. Это приводит к расхождению в декларируемых и реально преследуемых целях. Каждый актор также имеет в своем распоряжении стратегию формального присоединения без намерения реального исполнения принятых на себя обязательств. Подобная стратегия может дать отдельным национальным акторам международное конкурентное преимущество («трагедия общин», предложенная британским экономистом У.Ф. Ллойдом в 1833 г. [Lloyd, 1980]). Возможности международного сообщества в части исключения таких стратегий весьма ограничены, в результате чего общий процесс характеризуется высокой степенью взаимного недоверия.

[1] Позиция России состоит в том, что киберпространство должно быть демилитаризовано и кибервойна исключена с помощью международного законодательства, позиция США сводится к тому, что в той или иной форме агрессивные действия в киберпространстве являются состоявшимся фактом и задачей международного закона должно быть создание норм, регулирующих военные действия в киберпространстве в соответствии со сложившимся военным и гуманитарным правом. Соответствующие заявления были сделаны спецпредставителем МИД РФ Андреем Крутских (https://www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2804288) и представителем Госдепа США Мишель Маркофф (https://findit.state.gov/search?utf8=%E2%9C%93&affiliate=dos_stategov&sort_by=&query=statement+on+UN+GGE+2017)

Балансирующим осознанием является предвосхищение возможности существенной международной дестабилизации, которая будет иметь для отдельных акторов более опасные последствия, чем следование согласованным правилам. Однако в целом современное международное право не носит такого всеобъемлющего характера, как национальные законодательства. Всегда имеется возможность оставить ту или иную область неурегулированной, что предпочтительнее присоединения к законодательству, нарушающему национальные интересы.

Успешно заключенные и исполняемые международные договоры[1] в результате сводились к (1) гармонизации национального законодательства в областях с давно сложившейся практикой (например – торговое право); (2) созданию норм в отношении действий, имеющих потенциально катастрофические гуманитарные последствия (законы о ведении войны, ограничение ядерных испытаний, запрет химического и бактериологического оружия[2]), или (3) имеющих относительно небольшое значение для национальных интересов (конвенции по космическому пространству и Антарктиде[3]). Определенным исключением является международное морское право. Оно создавалось в необычной ситуации, когда страны с относительно небольшим общим весом в международном пространстве оказались в силу географии владельцами важнейшего ресурса – морских проливов, что давало им достаточно сильную переговорную позицию.

Киберпространство по своей природе отличается от всех перечисленных случаев. Оно возникло относительно недавно и находится в процессе постоянных изменений, что исключает обращение к сложившимся обычаям и практикам. Гуманитарные последствия злоупотреблений в киберпространстве – хотя и значительные – не выглядят сопоставимыми с ядерным, химическим или биологическим конфликтом. В то же время киберпростанство стало одним из ключевых драйверов социально-экономического и политического развития практически во всех странах мира, и это его значение постоянно растет. При этом архитектура нынешнего киберпространства дает существенное преимущество ограниченной группе стран (если не сказать, одной стране). У «малых» участников процесса нет и не предвидится никаких «балансирующих» возможностей для усиления своей позиции. Крупные страны-акторы могут извлечь существенную выгоду из неприсоединения или формального, но не соблюдаемого присоединения к регулированию[4]. В результате создание эффективного, исполняемого, согласованного регулирования киберпространства является задачей

[1] См. список ключевых договоров под эгидой ООН: https://www.un.org/en/sections/issues-depth/international-law-and-justice/index.html

[2] При этом участники соответствующих конвенций продолжали подозревать других участников в их нарушении, ряд нарушений конвенции в отношении химического оружия доказанно имел место (к примеру, ирано-иракская война 1980–1988 гг.) без серьезных немедленных последствий для нарушителей.

[3] В последнем случае присоединение к конвенции не мешает таким странам, как Аргентина и Чили, официально считать часть Антарктиды суверенной территорией.

[4] Примером является позиция Китая, проигнорировавшего Будапештскую конвенцию по киберпреступности, криминализировавшую определенные нарушения в области интеллектуальной собственности, для разрешения ситуации США потребовалось заключение отдельного двустороннего договора в 2015 г.

беспрецедентной сложности с юридической и технической, но прежде всего – с политической стороны.

Осознание всех этих сложностей породило ряд дискуссий в мировой юридической литературе, которые группируются вокруг двух тем: «Является ли международное право действительно правом?»[1] и «Является ли международное право действительно международным?». По первому пункту достаточно радикальная точка зрения была высказана в 1994 г. Ширли Скотт, которая заметила, что «определяющей послевоенной парадигмой в международных отношениях был реализм, который отвергает международное право как практически не имеющее отношения к вопросам “высокой” политики». По ее мнению, последняя в целом основывается на концепции «силы» [Scott, 1994]. Второй дискуссии посвящена, например, книга [Roberts, 2017].

Действительно, необходимо учитывать, что международное законотворчество в любом случае происходит не «с нуля», а оказывается вписанным в тот или иной исторический контекст. Возникновение Интернета как глобального феномена почти совпало по времени с моментом окончания холодной войны и распада «социалистического лагеря». Его развитие происходило параллельно со сложными политическими процессами 1990–2000-х годов. В связи с этим идеологемы времен холодной войны продолжают в большой степени определять взгляды ключевых стейкхолдеров мирового киберпространства на интересы, мотивы и стратегии оппонентов.

Различия в подходах между основными государствами-стейкхолдерами мирового киберпространства неоднократно становились предметом анализа как в отечественной [Зиновьева, 2016; Захаров, 2018], так и в зарубежной литературе [Kerttunen, Tikk, 2018]. Однако данный анализ, как правило, ограничивался ситуативно-техническим рассмотрением разногласий без выяснения их глубинных причин. Цель данной статьи состоит в том, чтобы проанализировать позиции ключевых стран – участниц дискуссий по вопросам международного регулирования киберпространства в контексте сложившейся культуры решения конфликтов частного и общественного. Результаты исследования помогают прийти к более глубокому пониманию позиции оппонентов и формулировать более реалистичные ожидания в отношении возможностей достижения согласия в области международного киберрегулирования.

## Метод анализа

Решение поставленной задачи включает, прежде всего, анализ ключевых документов, выражающих позиции сторон в дискуссии по международному регулированию, идущей на протяжении более 20 лет. Принципиально важно вписать эти документы в более широкий контекст взглядов на

[1] «Is international law really a law?», что можно также перевести как «Является ли международный закон действительно законом?», понятийные поля английского термина Law и российских «право» и «закон» пересекаются довольно сложным образом.

государственное управление. Всякий подход к регулированию должен имплицитно или эксплицитно учитывать расстановку приоритетов между частными и общественными интересами в сфере международных информационных сетей и возможную программу действий, создающих приемлемый баланс между этими интересами.

Официальная позиция России по вопросам международного кибер-регулирования сформулирована в представленном в ООН в 2011 г. проекте Конвенции об обеспечении международной информационной безопасности [МИД РФ, 2011], который стал своего рода итогом целой серии инициатив в формате ООН. Хотя формально проект был внесен группой стран, включающей также такого важного стейкхолдера глобального киберпространства как Китай, документ позиционировался как инициатива РФ и был воспринят именно в таком качестве в международной экспертной среде [Kerttunen, Tikk, 2018].

Основным оппонентом российской инициативы в ООН являются США [Демидов, 2013[1]; Хужина, 2015; Захаров, 2018; Prakesh, Baruah, 2014]. К их единомышленникам («like-minded powers») относят Великобританию и Нидерланды [Kerttunen, Tikk, 2018, p. 24]. Суть оппозиции состоит не в предложении сопоставимого альтернативного документа (поскольку поддерживаемая условным «Западом» Будапештская конвенция Совета Европы[2] о киберпреступлениях 2001 г. носит гораздо более ограничивающий характер)[3], а в отвержении самой идеи эффективной глобальной киберконвенции.

Официальным документом, описывающим ключевые подходы США к международному киберрегулированию, является «Международная стратегия в отношении киберпространства» 2011 г. [White House, 2011]. В этом документе излагаются взгляды администрации Барака Обамы на роль киберпространства в социально-экономическом развитии на национальном и глобальном уровне, а также цели и принципы действия США в отношении киберпространства. В 2018 г. администрацией Дональда Трампа была принята «Национальная стратегия в отношении киберпространства», описывающая в большей степени действия в отношении внутреннего пространства (homeland), однако затрагивающая и международный контекст. Важными дополнениями для анализа позиции

[1] В частности, было верно отмечено, что есть значительные расхождения между понятием «информационная безопасность», содержащимся в документе и носящим весьма широкий характер, и многими распространенными трактовками содержания «кибербезопасности», сводящегося к функционированию инфраструктуры компьютерных сетей. По словам автора, «конкуренция России и ее союзников (КНР и другие государства ШОС) с западными государствами в части утверждения на глобальном уровне того или иного понимания роли ИКТ в контексте международной безопасности приобретает черты идеологического противостояния» [Демидов, 2013, с. 137].

[2] Несмотря на то что Конвенция разработана Советом Европы, она открыта для присоединения всех стран. Из крупных неевропейских стран конвенцию ратифицировали на настоящий момент США, Канада, Австралия, Япония и Израиль.

[3] Россия была последовательным критиком Будапештской конвенции, считая, что она, с одной стороны, не носит достаточно всеобъемлющего характера в описании информационных угроз, а с другой стороны, не уважает национальный суверенитет участников (РИА «Новости», «РФ поддерживает разработку конвенции по борьбе с киберпреступностью», 28 октября 2014 г., https://ria.ru/20141028/1030552154.html)

США и их единомышленников являются заявления официальных лиц, сделанные на площадках международных организаций или адресованные СМИ.

Альтернативный «западный» подход к глобальному киберпространству представляет «Международная стратегия в отношении цифрового пространства» Франции [Ministere de l'Europe, 2018]. Эту страну не относят к непосредственному кругу единомышленников США, и в ее стратегии выражается озабоченность по поводу американской цифровой гегемонии. Также немаловажно, что французская «континентальная» правовая культура традиционно противопоставляется англо-американскому обычному праву.

Наконец, позиция одного из основных стейкхолдеров мирового киберпространства, Китая, выражена в принятой в 2017 г. «Национальной стратегии по сотрудничеству в кибепространстве» [Xinhua …, 2017].

Дополнительный контекст исследования задают проекты международного киберрегулирования, созданные частными лицами и организациями преимущественно в рамках «западной» части цифрового пространства, а также ряд инициатив крупных международных корпораций, призванные синхронизировать подходы в области создания безопасных цифровых систем [Stadnik, 2018]. Отдельный интерес представляют две редакции так называемого «Таллиннского руководства по международному закону, применимому к кибервойне» (во второй редакции слово «кибервойна» (cyber warfare) было заменено на «кибероперации» (cyber operations) [Schmitt, 2013; Schmitt, 2017]. Данные документы являются академическими исследованиями, представляющими мнение коллектива видных международных юристов о применимости существующих норм международного права к военным действиям в киберпространстве.

Для достижения цели исследования необходим инструмент комплексного сравнительного анализа перечисленных текстов. К сожалению, правовая компаративистика не имеет пока что единого признанного метода [Van Hoecke, 2015]. Наиболее распространенный так называемый функциональный метод не выявляет расхождения между разными правовыми системами в понимании того, что является или не является проблемой. В частности, применение функционального метода к проектам международного киберрегулирования создает впечатление разногласий в отношении предлагаемых способов решения там, где имеет место более глубокий конфликт идеологий и правовых культур.

Возможное решение проблемы было предложено Г. Франкенбергом, занимавшимся сравнительным анализом национальных конституций. В его модели «конституционной архитектуры» различаются четыре уровня: права и принципы, ценности и обязанности, организационные меры и, наконец, правила конституционных изменений и интерпретации [Frankenberg, 2006]. Поскольку международное киберрегулирование можно представить как попытку создания «конституции гло-

бального киберпространства», данная модель вполне подходит для целей настоящего анализа. Наибольший интерес при этом представляют первые два уровня: прав и принципов, ценностей и обязанностей.

С учетом того, что с практической точки зрения важно, прежде всего, усилить позицию России в области международного киберрегулирования, в центре анализа находится проект конвенции по информационной безопасности, предложенный в ООН в 2011 г., и позиции других стран по отношению к нему.

## Результаты анализа

Модель Франкенберга позволяет выявить и формализовать существенные различия в правовых подходах ведущих стран-стейкхолдеров глобального киберпространства на уровнях принципов и ценностей.

### *Принципы*

Российский проект Конвенции по информационной безопасности содержит два ключевых принципа: (1) необходимость отдельного всеобъемлющего регулирования вопросов глобальной информационной безопасности в рамках единого документа и (2) организация глобального киберпространства как совокупности национальных киберпространств, управляемых государствами [МИД РФ, 2011, с. 2].

*Первый принцип* разделяется и некоторыми авторами альтернативных концепций киберрегулирования. Например, проект договора С. Шольберга имеет следующее вступление:

> «Киберпространство, будучи пятым общим доменом – после суши, моря, воздуха и космоса – требует координации, кооперации и правовых мер среди всех наций. Договор о киберпространстве или серия договоров на уровне ООН… должны стать каркасом (framework) для мира, справедливости и безопасности» [Schjolberg, Ghernaouti-Hélie, 2011, p. I].

Однако группа «США и единомышленники» не поддерживает данный принцип, о чем можно судить по мнению, высказанному министром иностранных дел Великобритании Уильямом Хейгом [Foreign and Commonwealth Office, 2012]. В качестве альтернативы У. Хейг предложил семь принципов сотрудничества между государствами, бизнесами и организациями в киберпространстве: 1) необходимость для правительств действовать в киберпространстве пропорционально и в соответствии с международным законом; 2) необходимость предоставить каждому способность доступа в киберпространство, включая навыки, технологии, уверенность и возможность; 3) необходимость пользователям киберпространства демонстрировать терпимость и уважение к различиям в языке, культуре и идеях; 4) необходимость обеспечить открытость киберпространства для инноваций и самовыражения, свободного обмена идеями и информацией; 5) необходимость уважения

индивидуальных прав на частную жизнь (privacy) и обеспечения необходимой защиты интеллектуальной собственности; 6) необходимость коллективно работать над решением в ответ на угрозу от онлайн-преступников; 7) продвижение конкуренции, обеспечивающей справедливый возврат от инвестиций в сети, услуги и контент [Foreign and Commonwealth Office, 2012].

Таким образом, налицо расхождение между стремлением создать всеобъемлющий, формализованный юридический документ и предложением действовать на основании достаточно ограниченного набора правил, более близкого по языку к политической декларации, чем к законотворчеству. Здесь несложно увидеть общее противоречие между «континентальной» правовой традицией, основанной на правовых кодексах, и англо-американского «обычного права», традиционно скептичного к кодификации.

Российская концепция создана в рамках правовой культуры, считающей, что кодификация – «наиболее совершенная форма развития законодательства», и что она создает «прочный каркас, на котором держится вся правовая материя той или иной отрасли… законодательства» [Рахманина, 2008, с. 32, 36]. Точка зрения обычного права может быть выражена следующим образом: «наличие кодекса не является ни необходимым, ни достаточным условием для достижения этих принципов [свободы, равенства и справедливости]» [Canale, 2009].

Какое-то время ряд правоведов в США в принципе отрицали необходимость создания отдельного регулирования для Интернета, указывая, что практически все связанные с ним проблемы могут быть решены в рамках обычного права. Так называемая дискуссия о «лошадином праве» велась заочно между Ф. Истбруком [Easterbrook, 1996] и Л. Лессигом [Lessig, 1999] в конце 1990-х годов. Позиция первого состояла в том, что отдельное киберправо имеет не более смысла, чем отдельное «лошадиное право» (Law of the Horse), поскольку все необходимые нормы (владение, купля-продажа, правила движения и т.д.) уже содержатся в общем праве. Второй указывал, что киберпространство является более сложным феноменом, его отдельное регулирование необходимо и более того, фактически уже осуществляется изнутри самого киберпространства (см. ниже). Точка зрения Лессига достаточно скоро стала доминирующей – уже в 2001 г. США активно поддержали Будапештскую конвенцию о киберпреступности. Однако сама дискуссия, проходившая на площадках ведущих юридических форумов и журналов, показывает, что специальная кодификация не является правовым инстинктом в рамках англо-американской традиции.

США настаивают, что объем специального регулирования, осуществляемый в рамках Будапештской конвенции, вполне достаточен и не требует существенного расширения. В свою очередь, авторы Таллинских руководств в целом убедительно справляются с задачей интерпретации существующих международных норм, включая гуманитарное право и законы войны, в применении к военным операциям в киберпространстве.

В 2011 г. США окончательно сформулировали свою правовую позицию в отношении к международному киберпространству:

> «Разработка норм поведения государств в киберпространстве не требует переизобретения обычного международного права и не делает существующие международные нормы устаревшими… уникальные атрибуты сетевых технологий требуют дополнительной работы по выяснению того, как применять эти нормы и какое дополнительное понимание может быть необходимо для их расширения» [White House, 2011, p. 9].

*Второй принцип* российского подхода к международной информационной безопасности (конструирование глобального киберпространства через национальные) также находит понимание у ряда зарубежных авторов. В частности, он разделяется в проекте С. Шольберга, который в значительной мере основан на его опыте сотрудничества с Международным телеграфным союзом (ITU), пытающимся стать центральным международным агентством по управлению глобальным Интернетом (аналогично существующей практике в области телеграфной и телефонной связи).

Однако данный принцип вступает в противоречие с исторически сложившейся архитектурой Интернета, который задумывался как открытое мультистейкхолдерное пространство, в котором суверены присутствуют на равных правах со всеми участниками[1]. Формирование киберпространства происходило в рамках определенной идеологии, наиболее ярким выражением которой была «Декларация независимости киберпространства» американского поэта и политического активиста Джона Перри Барлоу:

> «Я объявляю глобальное социальное пространство, которое мы строим, естественным образом независимым от тирании, которую вы [правительства мира] стремитесь нам навязать. Вы не имеете морального права управлять нами, у вас также нет никаких методов правоприменения, которых нам стоит бояться. Правительства получают законную власть через согласие управляемых. Вы не искали от нас такого согласия и не получали его. Мы вас не приглашали… Киберпространство не лежит в ваших границах. Не думайте, что вы можете построить его… Вы не можете. Это явление природы, и оно растет само по себе через наши коллективные действия» [Barlow, 1996, p. 1].

При всей декларативности этого манифеста он содержит важные указания на то, что архитектура (или природа) цифрового пространства, действительно, создает почти непреодолимые препятствия для его регулирования правительствами. Киберанархизм имеет глубокие корни в

[1] Выделение в свое время домена. gov для государственных организаций ставило их в один ряд с образовательными учреждениями -. edu – и коммерческими компаниями -. com. Формальное наличие страновых доменов не создает достаточных оснований для национального суверенитета (вопреки мнению Уерпманна-Уитзака [Uerpmann-Wittzack, 2010, с. 1256]), поскольку значительное количество ведущих интернет-ресурсов зарегистрировано в межстрановых доменах, число которых было существенно расширено начиная с 2013 г.

движении хакеров, сложившемся в конце 1970-х годов[1]. В книге С. Леви «Хакеры. Герои компьютерной революции» отмечается, что многие из видных компьютерных активистов того времени перекладывали в киберпространство идеи хиппи 1960-х[2] [Levy, 1984].

Как указывает Лессиг, архитектура является одной из модальностей регулирования (наряду с законом, обществом и рынком). Поэтому в момент, когда Интернет привлек внимание государственных регуляторов, он уже эффективно регулировался изнутри. Таким образом, для кардинального изменения модальности регулирования киберпространства необходима, прежде всего, перестройка его архитектуры. По словам Лессига, «…хотя определенные версии киберпространства сопротивляются эффективному регулированию, это не означает, что любая версия киберпространства будет делать то же самое. Или, иначе, возможны версии киберпространства, в которых поведение будет регулироваться, и правительства могут предпринять шаги по усилению этой регулируемости» [Lessig, 1999, p. 506].

Такие идеи фактически были реализованы в достаточно многочисленных проектах создания «управляемого национального Интернета». Прежде всего, это «Великий файрволл» Китая, а также Иран, Туркменистан и т.д., не говоря уже о многочисленных случаях временных мер по ограничению Интернета, принимавшихся правительствами разных стран. Проблема состоит в том, что подобные ограничения неизбежно ставят национальных пользователей в неравные конкурентные условия на глобальном рынке, что является чувствительным для бизнеса и образовательных организаций. Развитые и успешные закрытые национальные сети, вроде французской Minitel, проиграли в свое время рыночную конкуренцию Интернету именно по причине его функционального превосходства [Орловский, Коровкин, 2020].

«Государствоцентричность» подхода российской концепции представляется слабостью даже тем аналитикам, которые в целом ей симпатизируют. Так, О. Демидов указывает, что «логика концепции Конвенции не позволяет документу охватить субъектов, которые в общем-то наполняют мировую систему коммуникаций содержанием и без которых информационный обмен невозможен» [Демидов, 2013, с. 140]. Однако расширить охват с тем, чтобы отразить в нем мультистейкхолдерную модель управления киберпространством невозможно с юридической точки зрения. Это фактически наделило бы субъектов внутригосударственного права разных государств международной правовой субъектностью [Пазюк, 2012, с. 238]. По этой причине реализация российского

[1] Тогда слово «хакер» не имело негативных коннотаций и использовалось для программистов, умеющих решать нестандартные задачи, связанные с организацией компьютерных сетей в условиях неразвитой инфраструктуры. Хотя часть хакеров пользовались несанкционированным доступом к телефонным сетям и довольно свободно относилиась к интеллектуальной собственности, их действия не имели конечной цели нанесения ущерба.

[2] В какой-то мере продолжение этих идей можно проследить в движении за создание децентрализованных криптовалют, основанном на манифесте Сатоши Накамото (псевдоним).

подхода в отношении глобального киберпространства требует де-факто национализации ряда институтов, составляющих сейчас архитектуру Интернета.

Российская правовая школа смотрит на национализацию следующим образом: «…институт национализации необходим для обеспечения поступательного экономического развития страны… позволяет преодолеть индивидуализм участников гражданско-правовых отношений и провести идею общественного интереса (общеполезности, общего блага, публичного интереса)» [Щенникова, 2012][1]. В противоположность этому современная англо-американская правовая школа фактически отказывается рассматривать национализацию как институт, считая ее возможной лишь в качестве чрезвычайно исключительной временной меры (economic emergency) [Davidson, 2014]. Таким образом, архитектурная перестройка глобального киберпространства, необходимая для его организации в виде совокупности национальных киберпространств, представляется в настоящее время нереалистичной.

### *Ценности*

В самом простом выражении ценности задают степень важности вещей, событий или действий и через это определяют принятие сложных коллективных решений. При этом систему ценностей, присущих той или иной культуре, вполне можно реконструировать из анализа развернутых текстов, вычленяя в них центральные понятия.

Подобный анализ российского проекта Конвенции по международной информационной безопасности позволяет выделить следующие концепты, составляющие ценностный каркас документа [МИД РФ, 2011]:

- государственный суверенитет;
- безопасность и стабильность;
- традиционность.

По мнению специалистов, предложенный проект во многом является развитием идей, содержащихся в российских внутренних стратегических документах, применительно к международному праву. А сама ценностная конструкция «суверенитет – стабильность – традиционность» представляет собой перенесение в киберпространство идеологии «суверенной демократии», сформулированной в 2006 г. В. Сурковым (тогда заместителем главы Администрации Президента РФ), которая постепенно превратилась в доминирующую идеологему, предельно редко оспариваемую в отечественном публичном мейнстриме.

[1] При этом, однако, национализацию в России называют спящим институтом в силу отсутствия необходимого законодательства, закон о национализации разрабатывался на протяжении ряда лет, но так и не был принят, в частности в ноябре 2019 г. Госдума большинством голосов отвергла законопроект, предложенный КПРФ. (ИА Regnum, «Госдума отказалась принимать закон о национализации имущества», 12 ноября 2019 г., https://regnum.ru/news/economy/2775635.html).

По отдельности перечисленные ценности разделяются многими участниками глобального киберпространства. Так, китайская «Стратегия по сотрудничеству в киберпространстве» ставит суверенитет на второе место после «мира» в ряду основополагающих принципов, а «защиту суверенности и безопасности» на первое место среди целей. Французская стратегия также обращает внимание на вопросы суверенитета и уделяет заметное внимание сохранению культурной идентичности (прежде всего, путем продвижения в Интернет франкоязычного контента). Признание важности «безопасности» как таковой лежит в основе всех дискуссий по киберрегулированию. Однако ни одна из крупных стран-стейкхолдеров мирового Интернета не оперирует описанной ценностной конструкцией, когда суверенитет государства, стабильность и традиционность рассматриваются как тесно связанная группа концептов.

Подход «США и единомышленников» основан на существенно другой ценностной конструкции. Это не означает, что ценности российской концепции напрямую оспариваются. Просто им приписывается низкий приоритет относительно других ценностных концептов. Международная киберстратегия США 2011 г. открывается вступлением Барака Обамы, в котором утверждается, что «кибербезопасность – это не цель сама по себе, это обязательство, которое наши правительства и общества должны добровольно принять на себя, чтобы дать инновациям расцветать, развивать рынки и улучшать жизни» [White House, 2011].

В ценностях западного мира гораздо выше стоит динамизм – развитие и инновации, – отраженный в четвертом принципе У. Хейга или в следующей фразе из американской Международной стратегии для киберпространства: «США будут проводить международную политику в киберпространстве, которая усилит (empowers) инновации, развивающие нашу экономику и улучшающие жизни здесь и за границей» [White House, 2011, p. 4].

Аналогичным образом обстоит дело с государственностью как основой для суверенитета. Присутствие государства имеет смысл лишь в тех случаях и в той мере, в какой мультистейкхолдерная модель оказывается неэффективной в достижении общественного блага. До тех пор, пока правительства западных стран не видят неустранимых провалов, проистекающих из существующей модели управления киберпространством, они не видят причин вмешиваться. Отсутствие государства в центре ценностной модели почти автоматически исключает важность суверенитета как концепции.

Основной ценностью «западного» подхода является идея равенства всех участников киберпространства, с особенным уважением к коммерческим и академическим игрокам, непосредственно создавшим его. В этом проявляется как ценностный компонент, проистекающий из американского конституционного права на «стремление к счастью» (pursuit of happiness), так и исторически сложившийся мессианизм США, тесно связанный с ценностями свободы и открытости. «Прави-

тельства, которые уважают права своих граждан, не имеют причин бояться свободного Интернета»[1] [Pozner, 2011]. По словам У. Хейга, «существует растущее расхождение мнений и действий между странами, ищущими открытого будущего для Интернета, и теми, кто движется по пути государственного контроля. Мы верим, что недостаточно просто работать с угрозами в области экономики и безопасности без сохранения открытости и свободы, на которых основан его [Интернета] успех» [Foreign & Commonwealth Office, 2012].

Ценности открытости и свободы являются основополагающими и для французской киберстратегии.

Альтернативный ценностный каркас подхода к киберрегулированию США и их единомышленников можно сформулировать как «динамизм (инновации) – равенство всех участников (вплоть до принижения роли государства) – открытость (архитектурная и содержательная)». Несложно видеть, что он противоречит ценностям российской концепции. Однако придание этому противоречию чисто инструментальной перспективы – предположение, что оно является лишь переговорной позицией – глубоко ошибочно. Представители западного действительно не могут оперировать иной картиной мира. В свою очередь, и они глубоко ошибочно приписывают российской концепции лишь тактические цели, не осознавая ценностной конструкции, стоящей за ней.

### *Типология подходов к киберрегулированию*

Полученные результаты согласуются с существующими типологиями отношений государства и общества. Так, Спенсер, Мурта и Линуэй в начале 2000-х годов применили к анализу роли государства в создании новых (инновационных) индустрий классификацию, предложенную Р.Л. Джепперсоном [Jepperson, 2000]. Тот выделил два измерения: тип коллективной агентской структуры (насколько «государственным» является общество) и тип организации общества (насколько оно «корпоративно»), что образовывало четыре возможных квадранта: 1) социальное корпоративное государство; 2) корпоративное государство; 3) либеральное плюралистское государство; 4) государственная нация [Spencer, Murtha, Lenway, 2005, p. 326].

В данной типологии США относились авторами к либерально-плюралистическим государствам. Россия (и другие незападные страны, за исключением Японии) ими не рассматривалась, однако она явно подходит под описание типа «государственная нация». Эти два типа не являются диаметрально противоположными. Они схожи по измерению организации общества – отсутствию сильных негосударственных институтов – «корпораций» в широком смысле слова (включая разного рода профессиональные ассоциации, академические сообщества и т.д.).

[1] Разумеется, это видение не разделяется во многих других странах мира. По мнению Захарова, «США используют угрозы и подкуп, склоняя к собственному пониманию демократии и неолиберальной экономической политики» [Захаров, 2018, с. 133], это утверждение отчасти справедливо, однако опять-таки приписывает инструментальный характер (удержание технического превосходства) действиям, имеющим ценностную природу.

Несколько иная типология может быть предложена, если в качестве измерений использовать роль государства в экономической (государство-организатор и государство-регулятор экономики) и политической (государство – идеологический лидер и деидеологизированное государство) жизни [Korovkin, 2018]. При такой классификации Россия оказывается в категории «супергосударств» (лидирующая роль в экономике и политике), а США и их единомышленники – в строго противоположной категории «государство как сервис».

В обоих случаях видно, что расхождение позиций по международному киберрегулированию имеет под собой глубокие различия во взглядах на роль государства, его мандат действий и способы взаимодействия государства и различных общественных институтов, включая бизнес.

## Заключение

Г. Франкенберг указывал, что возможны четыре типа конституции: контракт, манифест, программа и закон [Frankenberg, 2006]. Эффективное международное право возможно лишь как контракт, так как оно требует согласия всех сторон, которое может быть получено лишь при наличии у них достаточно веских выгод. В случае, если зона согласия окажется слишком узкой, контракт вырождается в манифест – формально поддерживаемый всеми участниками, но не имеющий практических последствий в нормировании их действий. Это обстоятельство делает выработку международного законодательства чрезвычайно сложным процессом. Расхождения позиций сторон, безусловно, часто имеют инструментальную природу: стремление обеспечить нации наиболее выгодную конкурентную позицию на глобальных рынках. Однако эти же расхождения могут иметь под собой и более глубокую природу: различие правовых культур (и культур в широком смысле слова), выражающееся в несовместимости принципов и ценностей законотворчества.

Подобную несовместимость демонстрируют официальные материалы подходов к международному киберрегулированию России и США. В дальнейшем целесообразно дополнить исследование анализом позиций других важных стран-стейкхолдеров глобального киберпространства, например Японии или Индии.

Приходится констатировать, что имеющиеся культурные расхождения делают маловероятным достижение в обозримом будущем широкого международного консенсуса в области киберправа. Особую сложность здесь представляет мультистейкхолдерная архитектура киберпространства[1]. Вероятным сценарием является регионализация киберпространства, с созданием в нем союзов, основанных на взаимном доверии участников и единстве их взглядов на ключевые принципы киберрегулирования. Примерами таких союзов являются декларация ШОС, конвенция Африкан-

[1] В истории международного права уже есть пример провала попытки регулирования мультистейкхолдерной среды – долго осаждавшаяся конвенция ООН о транснациональных компаниях так и не была в итоге принята, вопрос постепенно ушел с повестки организации [Hedley, 1999].

ского союза по защите данных и законодательство по защите персональных данных ЕС. В какой-то мере глобальное киберпространство превращается в «лоскутное одеяло» норм и регулирований, затрудняющее действия добросовестных акторов (государственных и негосударственных), но открывающее недобросовестным многочисленные правовые лакуны и лазейки.

## Список литературы

*Демидов О.* Обеспечение международной информационной безопасности и российские национальные интересы // Индекс безопасности. – 2013. – № 1 (104), т. 19, – С. 129–168.

*Захаров Т.В.* Международное сотрудничество государств в сфере информационной безопасности и правовые подходы к его регулированию // Государство и право в новой информационной реальности. – 2018. – № 1. – С. 119–134.

*Зиновьева Е.С.* Перспективные тенденции формирования международного режима по обеспечению информационной безопасности // Вестник МГИМО-Университета. – 2016. – № 4(49). – С. 235–247.

*Коровкин В.В.* Национальные программы цифровой экономики стран Ближнего Востока // Ars Administrandi (Искусство управления). – 2019. – Т. 11, № 1. – С. 151–175.

МИД РФ Конвенция об обеспечении международной информационной безопасности (концепция) / Министерство иностранных дел Российской Федерации. – 2011. – URL: https://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/191666 (дата обращения 03.04.2020.)

МИД РФ Response of the Special Representative of the President of the Russian Federation for International Cooperation on Information Security Andrey Krutskikh to TASS' Question Concerning the State of International Dialogue in This Sphere // Официальный сайт МИД РФ. – 2017. – 29.06. – URL: https://www.mid.ru/en/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2804288

*Орловский В., Коровкин В.* От носорога к единорогу. Как провести компанию через трансформацию в цифровую эпоху и избежать смертельных ловушек. – М.: Бомбара, 2020. – 367 с.

*Пазюк А.В.* Понятие международного информационного права как комплексной отрасли современного международного права // Актуальні проблеми міжнародних відносин. – 2012. – Випуск 111 (Частина І). – URL: https://digital.report/ponyatie-informatsionnogo-prava/ (дата обращения 02.04.2020).

*Рахманина Т.Н.* Актуальные вопросы кодификации российского законодательства // Журнал российского права. – 2008. – № 4(136). – С. 30–39.

*Хужина А.В.* Правовая природа сети Интернет: вопросы регулирования // Вестник ЮУрГУ. Серия «Право». – 2015. – Т. 15, № 1. – С. 101–107.

*Щенникова Л.В.* Гражданско-правовая наука о национализации // Вестник Пермского университета. Юридические науки. – 2012. – № 4. – С. 179–186.

*Barlow J.P.* A Declaration of the Independence of Cyberspace 1996 // Electronic Frontier Foundation. – 1996. – URL: https://www.eff.org/cyberspace-independence (дата обращения 02.04.2020).

*Benedikt M.* Introduction // Cyberspace: first steps / Michael Benedikt (ed.). – Cambridge: MIT Press, 1991 a. – P. 1–25.

*Benedikt M.* Cyberspace: Some Proposals // Cyberspace: first steps / Michael Benedikt (ed.). – Cambridge: MIT Press,1991 b. – P. 120–138.

*Canale D.* The Many Faces of the Codification of Law in Modern Continental Europe // A History of the Philosophy of Law in the Civil Law World / D. Canale, P. Grossi, H. Hofmann (ed.). – Dordrech: Springer, 2009. – P. 135–183.

*Davidson N.M.* Nationalization and Necessity: Takings and a Doctrine of Economic Emergency // Brigham-Kanner Property Rights Conf. (October 27, 2014). – 2014. – (Fordham Law Legal Studies Research Paper; N 2515333). – URL: https://ssrn.com/abstract=2515333 (дата обращения 05.04.2020.)

Department of State Explanation of Position at the Conclusion of the 2016–2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security / Department of State. – 2017. – URL: https://www.state.gov/explanation-of-position-at-the-conclusion-of-the-2016–2017-un-group-of-governmental-experts-gge-on-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-sec/(дата обращения 05.04.2020).

Department of State International Law in Cyberspace, Remarks Harold Hongju Koh, Legal Advisor U.S. Department of State, USCYBERCOM Inter-Agency Legal Conference, (September 18, 2012) / Department of State. – 2017. – URL: https://2009–2017.state.gov/s/l/releases/remarks/197924.htm -un-group-of-governmental-experts-gge-on-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-sec/ дата обращения 05.04.2020).

*Easterbrook F.* Cyberspace and the Law of the Horse / University of Chicago Legal Forum. – 1996. – 207 p.

Foreign and Commonwealth Office An open internet is the only way to suPort security and prosperity for all: Foreign Secretary speech at the Budapest Conference on Cyberspace. – 2012. – URL: https://www.gov.uk/government/organisations/foreign-commonwealth-office-un-group-of-governmental-experts-gge-on-developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-sec/ (дата обращения 03.04.2020).

*Frankenberg G.* Comparing constitutions: Ideas, ideals, and ideology – toward a layered narrative // International Journal of Constitutional Law. – 2006. – Vol. 4, N 3. – P. 439–459.

*Hedley R.* Transnational Corporations and Their Regulation: Issues and Strategies // International Journal of Comparative Sociology. – 1999. – Vol. 40, N 2. – P. 215–230.

*Jepperson R.L.* Institutional Logics: On the Constitutive Dimensions of the Modern Nation-State Polities. – Florence: European University Institute, 2000. – URL: https://cadmus.eui.eu/handle/1814/1676 (дата обращения 05.04.2020.)

*Kerttunen M., Tikk E.* Parabasis. Cyber-diplomacy in Stalemate / Norwegian Institute of International Affairs. – 2018. – URL: https://www.nupi.no/en/Publications/CRIStin-Pub/Parabasis-Cyber-diplomacy-in-Stalemate (дата обращения 05.04.2020).

*Korovkin V.* A digitally transformed state // BRICS Business Magazine. – 2018. – Vol. 21, N 2. – P. 46–55.

*Levy S.* Hackers: heroes of the computer revolution. – Doubleday, 1984. – 464 c.

*Lessig L.* The Law of the Horse: What Cyberlaw Might Teach // Harvard Law Review. – 1999. – N 113. – P. 501–549.

*Lloyd W.F.* Lloyd on the Checks to Population // Population and Development Review. – 1980. – N 6(3). – P. 473–496.

Ministere de l'Europe et des Affairs Etrangeres Stratégie internationale de la France pour le numérique / Ministere de l'Europe et des Affairs Etrangeres de France. – 2018. – URL: https://ch.ambafrance.org/Strategie-internationale-de-la-France-pour-le-numerique (дата обращения 05.04.2020).

*Pozner M.* Internet Freedom and Human Rights // American Rhetoric. – 2011. – URL: https://www.americanrhetoric.com/speeches/michaelposnerinetfreedomhumanrights.htm (дата обращения 03.04.2020).

*Prakesh R., Baruah D.M.* The UN and Cyberspace Governance // ORF Issue Brief. – 2014. – N 68. – URL: https://www.orfonline.org/wp-content/uploads/2014/03/IssueBrief_68.pdf (дата обращения 05.04.2020).

*Roberts A.* Is International Law International? – Oxford: Oxford University Press, 2017. – 420 p.

*Schjolberg S., Ghernaouti-Helie S.* A Global Treaty on Cybersecurity and Cybercrime // AiTOslo. – 2011. – URL: http://pircenter. org/media/content/files/9/13480907190.pdf. (дата обращения 03.04.2020).

*Schmitt M.* Tallinn Manual on the International Law Applicable to Cyber Warfare. – Cambridge: Cambridge University Press, 2013. – 215 c.

*Schmitt M.* Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. – Cambridge: Cambridge University Press. – 2017. – 30 p.

*Scott S.V.* International Law as Ideology: Theorizing the Relationship between International Law and International Politics // European Journal of International Law. – 1994. – Vol. 5, N 3. – P. 313–325.

*Spencer J., Murtha T., Lenway S.* How Governments Matter to New Industry Creation // AMR. – 2005. – N 30. – P. 321–337. – URL: https://doi.org/10.5465/amr.2005.16387889 (дата обращения05.04.2020).

*Stadnik I.* A New Cybersecurity Diplomacy: Are States Losing Ground in Normmaking? // Russian Council on International Affairs. – 2018. – URL: https://russiancouncil.ru/en/analytics-and-comments/analytics/a-new-cybersecurity-diplomacy-are-states-losing-ground-in-norm-making/ (дата обращения 05.04.2020).

*Uerpmann-Wittzack R.* Principles of International Internet Law // German Law Journal. – 2010. – Vol. 11, N 11. – P. 1245–1263.

*Van Hoecke M.* Methodology of Comparative Legal Research // Law and Method. – 2015. – C. 1–35.

White House International Strategy for Cyberspace. Prosperity, Security, and Openness in a Networked World / Office of President of the United States. – 2011. – URL: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (дата обращения 0504.2020).

Xinhua International Strategy of Cooperation on Cyberspace 2017 // Xinhuanet.com. – 2017. – URL: http://www.xinhuanet.com//english/china/2017–03/01/c_136094371_2.htm (дата обращения 05.04.2020).

# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ФИНАНСОВОМ СЕКТОРЕ: КИБЕРПРЕСТУПНОСТЬ И СТРАТЕГИЯ ПРОТИВОДЕЙСТВИЯ


**Семеко Галина Викторовна**

Кандидат экономических наук, ведущий научный сотрудник Отдела экономики Института научной информации по общественным наукам РАН (ИНИОН РАН), (Москва, Россия).



***Аннотация.*** *Проблемы обеспечения информационной безопасности финансовых организаций в мире и России рассматриваются в контексте развития цифровых финансовых технологий. Анализируются экономический ущерб от противоправных действий злоумышленников для отдельных финансовых организаций и финансовой системы в целом, основные инструменты кибератак, динамика и особенности инцидентов информационной безопасности в России. Оценивается уровень защищенности информационной инфраструктуры и показаны основные уязвимости и недостатки систем защиты финансовых организаций. Характеризуется политика Банка России в сфере информационной безопасности, ее ключевые цели и направления действий.*



***Ключевые слова:*** *информационная безопасность; информационные угрозы; финансовый сектор; киберпреступность; политика Банка России в сфере информационной безопасности.*

**Для цитирования:** Семеко Г.В. Информационная безопасность в финансовом секторе: киберпреступность и стратегия противодействия // Социальные новации и социальные науки. – Москва: ИНИОН РАН, 2020. – № 1. – С. 77–96.

URL: https://sns-journal.ru/ DOI: 10.31249/snsn/2020.01.06

## Введение

Бурное развитие информационных и цифровых технологий отразилось на всех отраслях экономики, но особенно сильное влияние оно оказало на сектор кредитно-финансовых услуг. Инновационные финансовые технологии коренным образом меняют традиционные бизнес-модели, спектр финансовых услуг и продуктов, способ взаимодействия финансовых посредников с клиентами, механизмы осуществления платежных и других операций и т.д. Они создают многочисленные потенциальные преимущества как для продавцов финансовых продуктов и услуг, так и для их клиентов, в частности, позволяют облегчить доступ клиентов к финансовым продуктам и услугам, ускорить и повысить качество обслуживания, снизить транзакционные издержки, повысить эффективность операций и т.п.

Вместе с тем финансовые технологии создают новые риски в кредитно-финансовой сфере, в том числе затрагивающие информационную безопасность (или кибербезопасность). Предпосылками для повышения значимости проблемы информационной безопасности являются скорость развития цифровых финансовых технологий и увеличение масштабов компьютерной преступности в кредитно-финансовой сфере.

В рейтинге глобальных рисков Всемирного экономического форума (ВЭФ) проблема киберпреступности входит в первую пятерку. Международное экспертное сообщество зачастую ставит ее выше, чем даже терроризм и экологические проблемы. Киберугрозы постоянно развиваются, по мере того как киберпреступность приобретает все более сложный и транснациональный характер.

## Информационные угрозы и киберпреступность: глобальные тренды

Финансовый сектор, активно осваивающий самые современные цифровые и информационные технологии, является одним из самых привлекательных объектов для нападений киберпреступников. Среди киберугроз, которым подвергается финансовый сектор, основными, по версии международной консалтинговой компании Accenture, являются [Future cyber threats: 2019 extreme …, 2019, p. 4–5]:

– кража учетных данных и личных данных кредитно-финансовых учреждений и их клиентов;

– манипулирование похищенными из финансовых учреждений данными для получения финансовой или политической выгоды, что дестабилизирует финансовые системы и рынки;

– деструктивные вредоносные программы (malware), т.е. программное обеспечение, разработанное с целью нанесения урона отдельному компьютеру или целой сети, серверу. Подобные при-

ложения проникают в компьютерную технику и наносят прямой или косвенный ущерб атакуемой организации, например, нарушают работу компьютера или похищают личные данные пользователя;

– совершенствование методов кибертерроризма по мере развития новых технологий: злоумышленники для проведения своих кибератак используют технологии, которые внедряют финансовые организации;

– дезинформация, которая широко применяется в ходе целевых многоэтапных атак на финансовые учреждения и рынки.

На серьезность киберрисков для мировой финансовой системы указывает директор-распорядитель Международного валютного фонда (МВФ) Кристина Лагард. По оценкам МВФ, потери финансовых организаций от кибератак в среднем могут составлять несколько сот миллиардов долларов в год, что уменьшает прибыль банков и потенциально угрожает финансовой стабильности. Успешные атаки уже привели к утечкам данных, в результате которых воры получили доступ к конфиденциальной информации и совершили мошенничество. Например, в январе 2018 г. на японской критповалютной бирже Coincheck хакерами было похищено более 500 млн долл. [Lagarde, 2018].

Финансовый сектор особенно уязвим по отношению к кибератакам. Финансовые организации являются привлекательными объектами из-за их важнейшей роли как посредников в движении денежных средств. Успешная кибератака на одну организацию может быстро распространиться через многочисленные взаимосвязи, объединяющие финансовую систему. Тем более что многие организации все еще пользуются устаревшими системами защиты, которые не могут противостоять действиям киберпреступников. Успешная кибератака может иметь прямые существенные последствия в виде финансовых убытков, а также косвенные издержки, такие как ухудшение репутации.

В мировой практике финансовых учреждений зарегистрировано большое число киберинцидентов, имевших серьезные последствия. Преднамеренные злоумышленные действия сторонних лиц в отношении кредитно-финансовых учреждений направлены на получение несанкционированного доступа к данным их информационной системы, нарушение функционирования информационной системы и (или) системы защиты информации, изменение или разрушение цифровых активов [Перцева, 2018].

Эксперты Банка России указывают на мировую тенденцию к увеличению финансовых потерь от кибератак (17% всего объема кибератак в мире приходится на финансовый сектор) [Основные направления развития информационной …, 2019, с. 3]. Ежегодные убытки мировой экономики от кибератак составляют 1 трлн долл., а ущерб РФ достигает более 600 млрд рублей (0,64% ВВП РФ) [Борисова, Белоусов, 2019, с. 1332].

Кроме значительного экономического ущерба, кибератаки приводят к изменениям в геополитических отношениях и снижению уровня доверия к сети Интернет и в конечном счете могут спровоцировать финансовый кризис.

К ключевым рискам в кредитно-финансовой сфере эксперты Банка России относят: финансовые потери клиентов (потребителей финансовых услуг), которые подрывают доверие к современным финансовым технологиям; финансовые потери отдельных финансовых организаций, которые могут отрицательно воздействовать на их финансовое положение; нарушение надежности операционной деятельности и непрерывности предоставления финансовых услуг, что может нанести ущерб репутации финансовых организаций и способствовать усилению социальной напряженности в обществе; возникновение системного кризиса из-за значимых для финансового рынка инцидентов информационной безопасности [Основные направления развития информационной ..., 2019, с. 3].

Расширение киберпреступности приводит к увеличению затрат финансовых учреждений на предотвращение и ликвидацию последствий противоправных действий злоумышленников. В мире отмечается постоянный рост таких затрат. Об этом, в частности, свидетельствует очередное (девятое) исследование компании Accenture, посвященное расходам компаний на борьбу с киберпреступностью. Оно основано на опросе 2647 топ-специалистов в области информационной безопасности из 355 организаций 11 стран (Австралия, Бразилия, Канада, Франция, Германия, Италия, Япония, Сингапур, Испания, Соединенное Королевство и США) [The cost of cybercrime ..., 2019]. Специалисты оценивали прямые затраты на выполнение данного вида деятельности и косвенные затраты, т.е. количество затраченных времени, усилий и других организационных ресурсов.

По итогам данного опроса, среднее количество кибератак в расчете на одну компанию выросло в 2018 г. по сравнению с 2017 г. на 17% (со 130 до 145) и на 67% за истекшие пять лет, а среднегодовые суммарные расходы на борьбу с киберпреступностью – соответственно на 12 (с 11,7 млн долл. до 13,0 млн) и 72%. По размеру среднегодовых расходов на борьбу с киберпреступностью лидировал банковский сектор (как и в предшествующие годы), где этот показатель составил в 2018 г. 18,87 млн долл. против 16,55 млн в 2017 г. Таким образом, прирост равнялся 14% [The cost of cybercrime ..., 2019, p. 10–12].

Традиционные стратегии по обеспечению кибербезопасности, как отмечалось на Международном конгрессе по кибербезопасности 2019 г. (ICC-2019), не защищают от целевых кибератак. Участники этого мероприятия – представители органов государственной власти, лидеры мирового бизнеса и ведущие эксперты по проблемам информационной безопасности – рекомендовали финансовым организациям уделять больше внимания разработке новых методов защиты и сотрудничеству с другими организациями – как с частными компаниями, так и с государственными струк-

турами. Одним из ключевых приоритетов стратегии обеспечения информационной безопасности финансовых организаций, по их мнению, должны стать действия, направленные на предвидение угроз и предупреждение атак. Кроме того, необходимо создать устойчивую к атакам систему управления информационной инфраструктурой и регулярно проводить мониторинг безопасности всего ее периметра [ICC 2019: Международный …, 2019, с. 23–25].

Чтобы вовремя распознавать киберугрозы и подготовиться к защите от них в будущем, финансовые организации, считают эксперты Accenture, должны разрабатывать проактивный план киберзащиты, основанный на моделировании кибератак [Future cyber threats: 2019 extreme …, 2019, p. 5].

## Киберпреступность в финансовом секторе: оценки экспертов

Расследованиями кибрепреступлений по всему миру занимается ряд международных компаний по предотвращению и расследованию киберпреступлений и мошенничеств с использованием высоких технологий. Они не только осуществляют сбор первичных данных об имевших место инцидентах информационной безопасности, но и проводят их анализ и делают прогнозы относительно потенциальных киберугроз.

Крупнейшим частным игроком на рынке расследований киберпреступлений в России является Group-IB, созданная в 2003 г. Она принимала участие в расследовании первых в России DDoS-атак, хищений средств с помощью вирусов для мобильных телефонов и целевых атак на банки. Сейчас ее деятельность вышла за пределы нашей страны. Компания имеет опыт расследования киберпреступлений по всему миру и сотрудничает с Интерполом и Европолом, а также с российскими провайдерами, специализирующимися на разработке программного обеспечения для финансовой сферы, защите информационных систем и т.д. Group-IB регулярно публикует результаты своих расследований.

В недавнем исследовании Group-IB [Hi-Tech Crime Trends 2019/2020 …, 2019] проанализированы глобальные тренды в развитии киберпреступности, а также активность наиболее опасных проправительственных хакерских групп и финансово мотивированных хакеров, целью которых являются шпионаж и саботаж. В целом за период со второй половины 2018 г. по первую половину 2019 г. были зарегистрированы активные действия 38 групп, из них семь были новыми.

Среди хакерских групп, атакующих банки по всему миру, большинство составляют русскоговорящие. Среди них выделяется «русскоязычная тройка» – Cobalt, Silence и MoneyTaker, первоначально «работавшая» на российском рынке, а в настоящее время осуществляющая географическую экспансию за рубежом, в частности в Индии, Вьетнаме, Пакистане, Таиланде, Чили, на Мальте и в других странах. В 2018 г., помимо «русскоязычной тройки», особенно активные атаки на банки по всему миру проводили северокорейская группа Lazarus и новая группа из Кении –

SilentCards. Целевые атаки на банки этих пяти хакерских групп представляют реальную угрозу финансовому сектору в мире.

В России каждый месяц отмечались успешные атаки в среднем на один-два банка, причем средний ущерб от таких инцидентов составил 132 млн руб./мес. (2 млн долл.). Эксперты Group-IB констатируют увеличение в три раза числа атак на банки с целью хищения средств через SWIFT.

Одной из наиболее опасных угроз для физических лиц остается мошенничество с банковскими картами, или кардинг (от англ. carding). В России объем рынка кардинга за анализируемый период оценивается в 663,4 млн долл. Большая часть скомпрометированных карт продается в специализированных «кардшопах». Ежемесячно в них загружается в среднем 686 тыс. текстовых данных карт [Обзор основных типов ..., 2019, с. 41].

С 2012 г. в России наблюдается снижение угроз со стороны банковских компьютерных троянов. Хотя в мире рынок Android-троянов продолжает развиваться, в России, после нескольких лет он прекратил свой рост, и число ежедневных хищений с помощью Android-троянов уменьшилось почти в три раза.

На международном рынке в 2018 г., в отличие от 2017 г., первую позицию среди атак на клиентов банка занял веб-фишинг[1]. По объему фишинговых сайтов мировым дилером являются США (80%), на втором месте – Франция, на третьем – Германия. В России ущерб от финансового фишинга в рассматриваемый период снизился на 65% (до 87 млн руб.), что в определенной степени стало следствием уменьшения количества активных хакерских групп и «средней добычи» от атаки [Hi-Tech Crime Trends 2019/2020 ..., 2019].

Эксперты Group-IB выявили за 2018 г. более 1,9 млн фишинговых ссылок, т.е. на 85% больше, чем в 2017 г. Из них свыше 26% ссылок приходилось на финансовый сектор. Жертвами финансового фишинга чаще всего были компании США (48% всех атак). На втором месте – Нидерланды (4,7%), далее идут Германия (4,51%) и Россия (4,46%) [Обзор основных типов ..., 2019, с. 35].

Ущерб от киберпреступлений с использованием вредоносного программного обеспечения (ВПО), или малвари (от англ. malware), которое нацелено непосредственно на банки и на их клиентов, по оценкам экспертов Group-IB, в России за период со второй половины 2018 г. по первую половину 2019 г. уменьшился на 85% (до 510 млн руб.) [Hi-Tech Crime Trends 2019/2020 ..., 2019]. Однако в России наблюдается рост числа преступлений против клиентов банков с помощью методов социальной инженерии и телефонного мошенничества, так называемого вишинга (от англ. vishing), который с конца 2018 г. охватил банковский рынок.

[1] Фи́шинг (от англ. fishing – «рыбная ловля, выуживание») – вид интернет-мошенничества с целью получения доступа к конфиденциальным данным пользователей – логинам, паролям и другой информации. Это достигается путем проведения массовых рассылок электронных писем.

Согласно другому исследованию Group-IB, посвященному анализу кибератак на российские кредитно-финансовые организации, 74% российских банков в 2018 г. были плохо подготовлены к хакерским атакам [Incident Response ..., 2019; Group-IB: более ..., 2019]. У трети финорганизаций имелись заражения вредоносными программами, а у половины были обнаружены следы атак, совершенных ранее. Серьезные недостатки отмечены в управлении банками своими сетевыми ресурсами. В частности, у 64% финорганизаций на согласование оперативных работ по киберинцидентам между подразделениями тратилось более четырех часов, притом что нормативное время составляет один час.

Банки оказались, по мнению экспертов, наиболее привлекательной целью для хакеров. На банковский сектор в 2018 г. приходилось около 70% хакерских атак, а остальная часть – 30% – в основном на компании топливно-энергетического комплекса и промышленные предприятия.

Эсперты Group-IB отметили также несогласованность в действиях внутренних подразделений банков и плохую организацию процедур по оценке источника вредоносного заражения, масштаба кибеинцидента и его локализации. У большинства финорганизаций, подвергшихся хакерским атакам, не был утвержден план реагирования на них, предусматривающий распределение задач между профильными подразделениями, сроки и методы противодействия злоумышленникам. Негативным моментом является и низкий уровень технической подготовки персонала. Так, в 70% организаций у персонала отсутствовали (или были недостаточными) навыки по поиску следов вредоносного программного обеспечения (ВПО) и не были проработаны процедуры по их выявлению.

Среди основных видов атак 2018 г. эксперты Group-IB выделяют целевые атаки, конкурентный шпионаж, вирусы-шифровальщики (ransomware – программы-вымогатели), криптомайнинг. При этом эксперты отмечают увеличение скорости и объемов обналичивания денег при атаках, нацеленных на кражу денежных средств: если три года назад вывод суммы в 200 млн руб. в среднем занимал около 25–30 часов, то в 2018 г. был зафиксирован случай, когда такая сумма была обналичена менее чем за 15 минут [Incident Response ..., 2019].

Атакованными оказываются финансовые организации разных размеров. Причем установлено, что устойчивость к кибератакам не связана напрямую с размерами банка, а в большей степени зависит от уровня профильной подготовки персонала и организации системы кибербезопасности в организации. Тем не менее лучшая техническая оснащенность крупных банков позволяет им эффективнее выявлять атаки и противодействовать им.

Ключевыми методами проникновения злоумышленников в сетевую инфраструктуру банков остаются фишинг и социальная инженерия. Как установили эксперты Group-IB, более 80% хищений денежных средств у клиентов банков в России производится с помощью методов социальной

инженерии. Например, мошенники звонят жертвам и представляются сотрудниками банка, предлагая услуги или сообщая об обнаружении подозрительной активности на их счетах [Incident Response ..., 2019]. Злоумышленники получают от клиентов их личные данные и коды доступа, а затем выводят все средства со счетов.

Одна из главных причин уязвимости банков – халатность сотрудников. Около 17% компаний, которые подверглись кибератаке и среагировали на нее, в дальнейшем вновь становились объектом нападения [Incident Response …, 2019]. В большинстве случаев причиной повторной атаки было неисполнение рекомендаций по устранению последствий первого киберинцидента, отмечают эксперты Group-IB.

Достаточно опасная тенденция, которая недавно получила развитие в мире, – это использование кибератак с целью нанесения урона репутации и вытеснения конкурента с рынка. Она особенно опасна для небольших банков, имеющих сравнительно низкий уровень информационной безопасности.

Одним из мировых лидеров в сфере комплексной защиты крупных информационных систем от современных киберугроз является международная компания Positive Technologies, основанная в России в 2002 г. Она специализируется на разработке программного обеспечения в области информационной безопасности, работает во многих странах мира и имеет региональные штаб-квартиры в Бостоне и Лондоне.

В последние годы Positive Technologies провела несколько исследований, посвященных проблемам кибербезопасности в кредитно-финансовом секторе России. Так, в недавнем исследовании проанализированы тактика и техника атак десяти организованных преступных групп, в том числе пяти групп, которые атаковали российские организации кредитно-финансовой сферы, и пяти других групп, которые выбирали в качестве жертв ведущие иностранные финансовые компании [APT-атаки на кредитно-финансовую ..., 2019]. Анализ базировался на опросе 306 респондентов, из которых 13% представляли финансовые организации.

Опрос, в частности, показал, что в 58% банков злоумышленник может получить доступ к тем или иным критически важным системам, в том числе к управлению банкоматами, межбанковским переводам, операциям с картами и т.д. Две трети опрошенных представителей финансовой отрасли (63%) указали, что на практике сталкивались с последствиями кибератак, а треть признали, что их организация понесла от кибератак прямые финансовые потери [APT-атаки на кредитно-финансовую …, 2019, с. 3–4].

По оценкам Positive Technologies, в России источником ВПО в финансовых организациях обычно являются фишинговые письма, тогда как за рубежом преступные группировки чаще используют другие методы внедрения в информационную систему финансовых организаций. При

этом три четверти российских банков не обладают достаточной способностью противостоять фишинговым атакам [APT-атаки на кредитно-финансовую ..., 2019, с. 7].

Еще одно интересное исследование Positive Technologies посвящено анализу защищенности корпоративной инфраструктуры финансовых организаций, банкоматов и онлайн-банков, торговых платформ, а также киберинцидентам в финансовом секторе [Защищенность кредитно-финансовой ..., 2019]. Согласно его результатам, кредитно-финансовый сектор входит в тройку наиболее часто подвергающихся хакерским атакам отраслей: первое и второе места занимают государственные и медицинские учреждения, на которые приходится по 19% всех атак, а атаки на финансовые организации составляют 11%. Целью большинства атак (65% инцидентов в 2018 г. против 92% в 2017 г.) является получение финансовой выгоды. Другая распространенная цель – получение информации о платежных картах, персональных данных, учетных данных пользователей для доступа к личным кабинетам (31% инцидентов в 2018 г. против 8% в 2017 г.).

Среди методов проникновения в сетевую инфраструктуру по итогам 2018 г. лидирует ВПО (58% атак). Далее по степени распространенности идут: социальная инженерия – 49% атак, хакинг[1] – 36, подбор учетных данных – 11 и эксплуатация уязвимостей веб-приложений – 5%. Такая структура методов атак в основном соответствует структуре 2017 г., хотя доля атак с использованием ВПО в 2017 г. была ниже (48%) [Защищенность кредитно-финансовой ..., 2019, с. 4].

Позитивным итогом 2018 г. стало то, что, несмотря на рост общего числа атак, доля успешных инцидентов была ниже, чем в 2017 г., а это означает сокращение финансового ущерба от них. Этому во многом способствовала деятельность Банка России, а также эффективная работа правоохранительных органов и арест участников крупных преступных группировок. Однако не стоит надеяться, что отмеченная тенденция продолжится в будущем. Скорее всего, произойдет перестройка преступных групп, появятся новые игроки на этом рынке, что спровоцирует рост числа атак.

Хотя уровень защиты внутреннего сетевого периметра банков несколько выше, чем в компаниях других отраслей, механизмы информационной защиты имеют многочисленные уязвимости. Они касаются управления учетными записями и паролями, обновления программного обеспечения, конфигурации аппаратного обеспечения (сервера), веб-приложений и т.д. Уязвимости конфигурации аппаратного обеспечения чаще всего связаны с несвоевременным обновлением программного обеспечения (67% банков) и хранением данных в открытом виде (58% банков). В управлении учетными записями и паролями особенно часто встречаются такие уязвимости, как использование словарных паролей (50% обследованных банков), открытых протоколов передачи данных (58%), доступные интерфейсы удаленного доступа и управления (50% банков). Уязви-

[1] Хакинг (от англ. hacking – взлом, атака) – внесение изменений в программное обеспечение для достижения определенных целей, очень часто изменения являются вредоносными.

мость веб-приложений обусловлена возможностью внедрения в них вредоносного SQL-кода[1] (33% банков) и загрузки произвольных файлов (25%), которые дают возможность выполнять произвольные команды на сервере [Защищенность кредитно-финансовой ..., 2019, с. 9].

Выявленные уязвимости внутренней сетевой инфраструктуры банков создают возможность кражи данных банковских карт и денег. В целом, как показало исследование, в 58% случаев защитный барьер банков не является преградой для проникновения злоумышленников. Более чем в половине случаев система защиты не может предотвратить кражу денежных средств в онлайн-банках [Защищенность кредитно-финансовой ..., 2019, с. 3].

Серьезной проблемой для большинства финансовых организаций является недостаточная осведомленность персонала в вопросах информационной безопасности. Как показало обследование компетентности персонала, в 75% банков сотрудники переходили по ссылке в фишинговом письме, а в 25% вводили свои учетные данные в ложную форму аутентификации. Более того, в 25% организаций сотрудники запускали на своем компьютере вредоносное вложение [Защищенность кредитно-финансовой ..., 2019, с. 11].

Как уже отмечалось, наиболее распространенным инструментом доставки ВПО является фишинг – большинство активных преступных группировок применяют его для проникновения во внутренний сетевой периметр банков. Это свидетельствует о высокой уязвимости сотрудников банков к методам социальной инженерии, используемым злоумышленниками.

Во всех обследованных в 2017–2018 гг. банках уровень безопасности внутренней сети, считают эксперты Positive Technologies, недостаточен для выявления и предотвращения проникновения с помощью кибератак. В 33% банков злоумышленники могут взломать сетевой периметр и получить доступ к управлению банкоматами, межбанковскими переводами, информации об операциях по банковским картам и т.д. [Защищенность кредитно-финансовой ..., 2019, с. 10]. Выявленные уязвимости и проблемы в системе безопасности банков, считают эксперты Positive Technologies, свидетельствуют о приоритетности задачи укрепления системы информационной защиты. Учитывая масштабность и сложность ее решения в рамках отдельной корпоративной сетевой инфраструктуры, эксперты рекомендуют финансовым организациям развивать сотрудничество с партнерами по бизнесу, обмениваться информацией о методах и последствиях атак, способах обнаружения и предотвращения угроз и т.д. Кроме того, безусловными приоритетами являются регулярный мониторинг внутренней сетевой активности, повышение уровня компетенции и осведомленности сотрудников в вопросах информационной безопасности.

[1] SQL (Structured Query Language – структурированный язык запросов) – язык управления базами данных для реляционных баз данных.

## Политика Банка России в сфере защиты информации

Хотя в России системно значимые кредитно-финансовые учреждения пока не подвергались кибератакам, которые способны нанести существенный ущерб, отдельные инциденты вызывали нарушение непрерывности предоставления финансовых услуг и усиливали социальную напряженность в обществе.

В последние годы задача обеспечения информационной безопасности финансовых организаций и развития устойчивой и защищенной цифровой инфраструктуры в России является одним из стратегических приоритетов Банка России. В своем выступлении в Совете Федерации глава Банка России Э. Набиуллина подтвердила намерение и дальше «усиливать надзор, стимулировать банки тщательно подходить к вопросам кибербезопасности». «Киберустойчивость – это не просто поставить на компьютер антивирусную программу, нужно писать требования киберустойчивости ко всем бизнес-процессам. Именно это критически важно для следующего динамичного развития технологий», – добавила она. К сожалению, российские банки и другие финансовые организации пока еще не научились управлять киберрисками: в ходе проверок банков на предмет киберустойчивости, которые проводил Банк России в 2019 г., было выявлено более 730 нарушений. Около 80% связаны с недостаточным уровнем информационной защиты в финансовых организациях [ЦБ выявил в банках ..., 2019]. Хотя пока обнаруженные проблемы не являются критическими, указала Э. Набиуллина на Международном конгрессе по кибербезопасности, в любой момент они могут стать таковыми, если их не решать [ЦБ обнаружил нарушения ..., 2019].

Ведущие российские банки не согласны с критикой Банка России. Они достаточно активно вкладывают средства в систему информационной защиты. Руководство Сбербанка России справедливо утверждает, что банковская отрасль «лучше готова к кибератакам по сравнению с большинством других российских отраслей». Наибольшим риском для клиентов Сбербанка России, согласно собранным его специалистами данным и проведенному анализу атак, являются новые способы социальной инженерии. Специальное подразделение Сбербанка России – центр реагирования на киберинциденты (SOC Сбербанка) – ежедневно регистрирует вредоносные вложения и фишинговые рассылки. Всего за 2018 г. на компьютеры Сбербанка поступило более 600 тыс. электронных писем, содержащих фишинг и вредоносные вложения. Каждую неделю Сбербанк отражал в среднем одну-две хакерские атаки на свои системы (всего 96 атак за 2018 г.) [Банки демонстрируют ..., 2019].

В отличие от крупных банков в остальных финансовых организациях, где нет достаточных финансовых и кадровых ресурсов, системы информационной защиты работают менее эффективно. По этой причине в мелких и средних финансовых организациях инциденты информационной

безопасности могут привести к прекращению их деятельности. И это уже серьезный повод для вмешательства регулятора.

За последние годы Банк России, опираясь на мировой опыт, предпринял ряд важных шагов, нацеленных на повышение информационной безопасности финансовой сферы. Так, регулятор разработал и вводит общие требования к информационной инфраструктуре банков, их программному обеспечению, системе хранения персональных данных, методам идентификации, криптографической защите данных и т.д. Банком России принят комплекс документов, описывающий единый подход к построению системы обеспечения информационной безопасности организаций банковской сферы с учетом требований российского законодательства – Стандарт Банка России по обеспечению информационной безопасности организаций банковской системы РФ (СТО БР ИББС). Он касается безопасности финансовых (банковских) операций, аутсорсинга, аудита, сбора и анализа данных при реагировании на кибератаки, оценки соответствия информационной безопасности организаций банковской системы требованиям и др. Внедрение Стандарта должно способствовать повышению доверия к банковской системе России и стабильности ее функционирования, использованию адекватных мер по защите от реальных угроз информационной безопасности, предотвращению и снижению ущерба от кибератак.

Важной инициативой Банка России стали создание новых структурных подразделений – Департамента финансовых технологий и Центра мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦерТ) – и последующее введение в эксплуатацию автоматизированной системы обработки информации о соответствующих инцидентах (АСОИ ФинЦЕРТ) и автоматизированной системы «Фид-АнтиФрод», обеспечивающей ведение базы данных о случаях и попытках осуществления переводов денежных средств без согласия клиента.

Для обеспечения сохранности банковских счетов и вкладов Банк России в 2019 г. ужесточил требования по защите средств банков и их клиентов от киберпреступников. Соответствующее положение Банка России, опубликованное 21 мая 2019 г., вменяет в обязанность кредитным организациям обеспечение информационной безопасности основных банковских операций (привлечение вкладов физических и юридических лиц, размещение привлеченных средств, открытие и ведение банковских счетов и др.). Для системно значимых банков, операторов платежных систем и кредитных организаций предусмотрены максимальные требования в отношении безопасности операций, а для остальных участников рынка – стандартные требования [Банк России расширил...].

В начале марта 2020 г. Банк России сообщил о том, что начинает штрафовать банки за отсутствие систем распознавания мошеннических операций. Речь идет о технологиях антифрода, позволяющих отслеживать нетипичные для клиентов операции, которые потенциально может совершать мошенник.

Анализом данных о компьютерных атаках на организации кредитно-финансовой сферы и на их клиентов в Банке России занимается специально созданное для этого в 2015 г. в Департаменте информационной безопасности подразделение – ФинЦЕРТ (центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере). Его задачей является организация взаимодействия Банка России с кредитными и некредитными организациями, разработчиками антивирусных программ, провайдерами связи, правоохранительными органами и другими заинтересованными сторонами с целью обмена информацией об угрозах информационной безопасности. Сотрудничество Банка России с заинтересованными сторонами основывается на соглашении об обмене информацией. Каждый участник информационного обмена имеет право в любой момент обратиться за помощью в ФинЦЕРТ при проникновении в его информационную сеть ВПО, попытках злоумышленников воспользоваться уязвимостями программного обеспечения его сети, подозрительных сетевых взаимодействиях и т.п. Важным источником сведений о кибератаках является также участие специалистов ФинЦЕРТ в соответствующих криминалистических расследованиях.

ФинЦЕРТ стал главным центром информации о совершенных кибератаках, их жертвах, виновниках, используемых мошенниками методах и т.д. Анализ собранных данных дает возможность оценить сложившуюся ситуацию в области киберпреступлений в финансовом секторе, масштабы преступных действий, выявить «слабые места» в программном обеспечении финансовых организаций, выработать рекомендации по эффективной защите корпоративных информационных сетей.

По итогам 2018 г. эксперты ФинЦЕРТ подготовили обзор, в котором суммируются данные о 687 атаках, в том числе о 177 целевых атаках[1], осуществленных на финансовые организации [Обзор основных типов …, 2019, с. 5]. Материалы обзора свидетельствуют о том, что основным методом распространения ВПО класса ransomware (программ-вымогателей, вирусов шифровальщиков) в 2018 г. были почтовые рассылки (53% всех вредоносных рассылок). Через рассылки осуществлялось распространение и так называемого финансового ВПО, конечной целью использования которого является хищение денежных средств (34% рассылок). Распространение ВПО в 2018 г. осуществлялось более чем через 540 ресурсов в сети Интернет, из которых свыше 500 находились за пределами РФ [Обзор основных типов ..., 2019, с. 6, 8].

К концу 2018 г., как показал анализ, наблюдалась переориентация наиболее опасных атак с российских финансовых организаций на организации ряда стран СНГ. Как и в предшествующем году, самым привлекательным объектом атак оставался процесс обработки онлайн-транзакций банковских карт. Распространенным объектом атак были также атаки на банковские устройства самообслуживания. Основную роль в атаках на клиентов (юридических лиц), как правило, играли

[1] Под целевыми атаками специалисты ФинЦЕРТ подразумевают атаки, направленные на получение финансовой выгоды и затрагивающие организации кредитно-финансовой сферы.

методы социальной инженерии, а не какие-либо технологически сложные инструменты. По расчетам, средний период между первичной компрометацией ИТ-системы финансовой организации до момента хищения составлял в среднем 20–30 календарных дней.

Атаки на финансовые организации обычно осуществляют хорошо организованные преступные группы, в состав которых входят организаторы, принимающие стратегические решения, квалифицированные программисты и инсайдеры кредитно-финансовой сферы (из числа действующих либо бывших сотрудников).

Среди инцидентов по распространению ВПО (375 инцидентов), зарегистрированных ФинЦЕРТ в 2018 г., 19% (71) приходилось на целевые атаки [Обзор основных типов ..., 2019, с. 10]. В проведении многих целевых атак подозреваются две основные организованные группы – Cobalt и Silence. Стратегия распространения ВПО, применяемая этими и другими группами, строится на рассылке фишинговых писем по электронным адресам сотрудников атакуемой организации. Если кто-то из сотрудников октрывает вложение письма, то автоматически происходят загрузка и запуск ВПО, которое обеспечивает злоумышленникам доступ к компьютеру. Для рассылки преступники обычно подменяют адрес отправителя, используя для этого специально созданный интернет-ресурс, почтовый ящик какой-либо организации или ранее скомпрометированный почтовый сервер. За последние годы, как признают эксперты, выросло мастерство преступников в составлении фишинговых писем, содержание и форма которых тщательно продумываются с учетом поставленной цели.

Целевые атаки, проведенные, как предполагает ФинЦЕРТ, группой Cobalt, нанесли в 2018 г. российским финансовым организациям ущерб в размере не менее 44 млн руб., а атаки группы Silence – более 14 млн руб. [Обзор основных типов ..., 2019, с. 14]. Хотя соответствующая сумма ущерба от этих групп в 2017 г. была значительно выше, не следует трактовать данный факт как тенденцию к сокращению риска целевых атак.

Атаки на клиентов финансовых организаций – юридических и физических лиц – различаются по своим характеристикам. Так, атаки на физических лиц менее сложны с технической и организационной точки зрения, обычно не нуждаются в высококвалифицированных исполнителях. Юридических лиц чаще атакуют организованные преступные группы, состав которых обычно нестабилен. Организованные группы больше склонны к частым изменениям в методах и объектах атак, которыми, как правило, являются программное обеспечение для платежных операций и сервисы электронной почты бухгалтерских и финансовых подразделений организаций. Новым способом внедрения ВПО в ИТ-системы организаций-клиентов банков, зафиксированным в 2018 г., ста-

ли так называемые «атаки на водопое» (watering hole)[1], т.е. заражение через скомпрометированный интернет-ресурс, который посещают эти организации.

Недостаточный уровень компьютерных знаний, халатность и беспечность сотрудников организаций-клиентов банков создают благоприятные условия для хакерских атак. В связи с этим, подчеркивают эксперты ФинЦЕРТ, информационная безопасность организаций в значительной степени зависит от эффективности действий их руководства в области повышения цифровой грамотности персонала и обучения сотрудников правилам безопасной работы с электронной почтой и с ресурсами Интернета. Кроме того, организации-клиенты должны своевременно обновлять антивирусные программы и повышать квалификацию своих специалистов в области информационной безопасности.

Злоумышленники-одиночки и небольшие хакерские группы с непостоянным составом в основном специализируются на атаках на банковские устройства самообслуживания. Как и в предшествующие годы, в 2018 г. они использовали атаки типа blackbox (подключение к диспенсеру банкомата устройства, например, портативного компьютера, которое отправляет команды для выдачи купюр) и типа «прямой диспенс» (установка и активация на банкомате ВПО, перехватывающего контроль функции выдачи наличных).

Существенно возросло в 2018 г. количество атак на финансовые организации с использованием программ-вымогателей, но среди них не было отмечено успешных и привлекших широкое внимание инцидентов. За период с сентября по декабрь 2018 г. было зафиксировано 195 попыток проникновения программ-вымогателей [Обзор основных типов ..., 2019, с. 25]. Главным каналом их распространения являются фишинговые письма, содержащие ВПО.

Комплекс мер, считают эксперты, может помочь финансовым организациям снизить риск кибератак. Это достаточно простые, но полезные и обязательные к исполнению действия, касающиеся использования (и своевременного обновления) антивирусного и офисного программного обеспечения, операционных систем, браузеров, приложений, учетных записей, а также контроля доступа пользователей к критичным ИТ-системам, проведения тренингов с сотрудниками организации и представителями клиентов и др. Если организация не в состоянии самостоятельно справиться с кибератакой, то эксперты рекомендуют привлекать структуры, компетентные в вопросах информационной безопасности.

Объем похищенных денежных средств со счетов юридических лиц-клиентов финансовых организаций, по данным обязательной отчетности об инцидентах информационной безопасности, поступающей от финансовых организаций в Банк России, в последние годы имеет тенденцию к

[1] Суть подобных атак состоит в том, что злоумышленники заражают вредоносными программами веб-сайты, часто посещаемые их потенциальными жертвами (хакеры поджидают жертв у «водопоя»). Это могут быть сайты компаний-партнеров или подрядчиков, общественных организаций и даже правительственных учреждений.

сокращению. Так, в 2018 г. сократился до почти 1,5 млрд руб. против около 1,6 млрд в 2017 г., 1,9 млрд в 2016 г. и 3,7 млрд в 2015 г. Противоположная динамика характерна для хищений с платежных карт, выпущенных российскими финансовыми организациями (около 1,4 млрд руб. в 2018 г. против почти 1,0 млрд в 2017 г., 1,1 млрд в 2016 г. и в 2015 г.) [Основные направления развития информационной ..., 2019, с. 3–4]. Хотя в общем объеме операций с платежными картами доля похищенных средств в России остается низкой по международным нормам – 0,0018% (т.е. на тысячу рублей переводов приходится 1,8 коп.). Для сравнения: Европейской службой банковского надзора (EBA) установлен более высокий допустимый порог этого показателя – 0,005% (т.е. 5 евроцентов на тысячу евро переводов).

Обзор ФинЦЕРТ по итогам инцидентов информационной безопасности, зафиксированных в 2019 г., свидетельствует, что проблема хищения денежных средств с помощью электронных средств платежа (включая банковские карты, системы дистанционного банкинга «Клиент-банк», электронные кошельки – Яндекс. Деньги, WebMoney и QIWI) остается крайне актуальной [Обзор операций, совершенных ..., 2020]. Для получения данных о хищениях средств со счетов физических и юридических лиц в 2019 г. была введена новая форма и методика отчетности о нарушениях защиты информации при переводах денежных средств (0403203 вместо формы 0409258)[1]. Предполагается, что это новшество позволит более полно отразить реальное положение дел в сфере хищения денежных средств киберпреступниками.

Анализ полученной от финансовых организаций информации показал, что в 2019 г. общий объем хищений со счетов физических и юридических лиц с помощью электронных средств платежа составил более 6,4 млрд руб. (всего 576,6 тыс. операций). При этом средний размер хищения в расчете на одну несанкционированную операцию по счетам юридических лиц равнялся 152 тыс. руб., а по счетам физических лиц – 10 тыс. руб. Причем в большинстве случаев (69%) преступники побуждали клиентов к самостоятельному совершению операции с помощью методов социальной инженерии. К сожалению, банки возместили клиентам лишь небольшую часть похищенного – около 15% [Обзор операций, совершенных ..., 2020, с. 4].

В общем объеме операций с использованием платежных карт доля операций без согласия клиентов (т.е. хищений) немного увеличилась в 2019 г. – до 0,0023% против 0018% в 2018 г. [Обзор операций, совершенных ..., 2020, с. 6][2]. Операции хищения совершались по трем основным ка-

[1] См. Указание Банка России от 30.03.2018 № 4753-У «О внесении изменений в Указание Банка России от 9 июня 2012 года № 2831-У "Об отчетности по обеспечению защиты информации при осуществлении переводов денежных средств операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных средств"» (Зарегистрировано в Минюсте России 01.06.2018 № 51248).

[2] Целевой показатель доли объема несанкционированных операций в общем объеме операций с использованием платежных карт, установленный Банком России на 2020 г., равен 0,005%.

налам – через банкоматы, терминалы и импринтеры[1] (7% от общего числа операций без согласия физических лиц и 9% от общего объема таких операций); оплата товаров и услуг в Интернете (соответственно 65% и 52%) и операции дистанционного банковского обслуживания (28% и 39%). Таким образом, лидером по числу и объему хищений с использованием платежных карт являются интернет-транзакции, а второе место занимают операции с использованием дистанционного банкинга. Однако по среднему размеру одного хищения (14 тыс. руб.) лидируют операции дистанционного банковского обслуживания, а интернет-транзакции находятся на второй позиции (8 тыс.) [Обзор операций, совершенных ..., 2020, с. 21].

В свою очередь, юридические лица в 2019 г. сообщили банкам о 4609 операциях без их согласия на общую сумму 701 млн руб. Доля компенсированных банками похищенных средств в случае с юридическими лицами была более низкой (10%), чем в случае с физическими лицами (15%). Также существенно более низкой (16%) была доля хищений средств со счетов юридических лиц с использованием методов социальной инженерии (против 69% операций физических лиц) [Обзор операций, совершенных ..., 2020, с. 13]. Злоумышленники осуществляли операции без согласия юридических лиц в основном через несанкционированный доступ к дистанционному банкингу и переводам денег по корсчетам юридических лиц.

В 2019 г. Банк России получил сведения от финансовых организаций о 973 случаях несанкционированного доступа к их информационной системе, в результате которых они понесли ущерб в размере почти 104 млн руб. Из них ущерб от компьютерных атак и несанкционированного доступа к информации о банковских счетах составил около 23 млн руб. (58 инцидентов) [Обзор операций, совершенных ..., 2020, с. 16].

Стратегия Банка России по обеспечению информационной безопасности кредитно-финансовой сферы закреплена в «Основных направлениях развития информационной безопасности кредитно-финансовой сферы на период 2019–2021 годов» (далее – Стратегия) [Основные направления развития информационной …, 2019]. В ней определены ключевые цели и задачи по обеспечению информационной безопасности и киберустойчивости в кредитно-финансовой сфере, а также подробно описаны мероприятия по их реализации. Выделены три уровня, на которых должна обеспечиваться информационная безопасность финансовых организаций – вычислительная инфраструктура, прикладное программное обеспечение и приложения (используемые технологии обработки данных). Основное внимание в Стратегии уделяется таким направлениям, как создание механизма правового обеспечения информационной безопасности; повышение защищенности информационной (вычислительной) инфраструктуры финансовых организаций; ликвидация уязвимостей прикладного программного обеспечения, применяемого для переводов денежных средств; совершен-

[1] Импринтер – механическое устройство, предназначенное для оформления слипа при совершении операции с платежной картой.

ствование технологий обработки данных; развитие финансовых технологий; подготовка специалистов в области информационной безопасности; расширение международного сотрудничества в области информационной безопасности и др. Одной из стратегических задач Банка России является также защита потребителей финансовых услуг от мошенничества и хищений средств.

Комплекс намеченных Банком России мероприятий в области информационной безопасности включает:

– совершенствование отраслевых стандартов и требований, касающихся технологической устойчивости, бесперебойности и безопасности применения финансовых технологий;

– разработка новых форм и методов взаимодействия и реагирования на информационные угрозы в рамках деятельности ФинЦЕРТ Банка России;

– повышение уровня технологической устойчивости, бесперебойности и безопасности при применении финансовых технологий, а также мониторинг состояния информационных систем финансовых организаций.

Поставленные задачи Банк России предполагает реализовывать на основе комплекса государственных стандартов, которые отражают требования к уровню защищенности финансовых (банковских) операций. Оценка соответствия информационной безопасности на каждом из выделенных уровней будет проводиться по определенным показателям (метрикам). А для анализа метрик намечено использовать технологии Big Data. В целях нейтрализации выявленных уязвимостей Банк России наметил разработать методологию расчета минимального размера финансового обеспечения, требуемого для покрытия потенциального ущерба. Кроме того, Банк России считает необходимым установить в нормативном порядке обязанность финансовых организаций предоставлять сведения о доле несанкционированных клиентом операций в общем объеме операций.

Методология оценки защищенности программного обеспечения и приложений предполагает разработку так называемого профиля защиты (или риск-профиля), который обобщает несколько групп показателей, характеризующих их соответствие требованиям безопасности в конкретной финансовой организации при банковских операциях, переводе денег и т.д. Профиль защиты позволяет оценить вероятность возникновения у конкретных финансовых организаций проблем в области информационной безопасности. При этом различаются три уровня защищенности финансовых организаций – минимальный, стандартный и усиленный. Для конкретных финансовых организаций уровень защищенности определяется с учетом вида их деятельности, специфики услуг, бизнес-процессов и технологических процессов; объема финансовых операций и значимости финансовой организации для финансового рынка и национальной платежной системы.

Необходимым условием обеспечения информационной безопасности является наличие квалифицированных кадров, в связи с чем Банк России планирует содействовать сотрудничеству ме-

жду вузами и финансовыми организациями. Развитие различных форм такого сотрудничества позволит модернизировать учебный процесс с учетом современных требований в области информационных технологий и информационной безопасности и в конечном счете готовить специалистов, способных своевременно и эффективно реагировать на преступные действия злоумышленников.

В связи с трансграничным характером киберугроз Банк России считает необходимым и дальше развивать международное сотрудничество в области кибербезопасности. В частности, намечено расширять участие экспертов Банка России в деятельности ряда международных организаций. Кроме того, Банк России считает необходимым взаимодействовать с центральными банками иностранных государств, в том числе и с регуляторами стран Евразийского экономического союза, а также с международными сообществами и национальными группами по реагированию на киберинциденты.

## Заключение

Финансовый сектор является одним из лидеров в вопросах использования информационных технологий. Одновременно он представляет собой приоритетную мишень для киберпреступников. За прошедшие годы киберпреступники стали значительно более организованными и опытными, а киберугрозы – более глобальными. Очевидно, что обеспечение информационной безопасности останется ключевым направлением развития в ближайшем будущем. Большинство финансовых организаций понимают серьезность киберугроз и последствия инцидентов информационной безопасности. Однако этого недостаточно, чтобы уменьшить ущерб от кибератак. Нужны активные действия по обновлению системы защиты, отслеживанию эффективности и надежности ее работы, повышению уровня квалификации персонала, сотрудничеству с клиентами и другими финансовыми организациями и т.д.

Приоритетное место проблемы информационной безопасности занимают и в стратегии отечественного регулятора – Банка России. Положительным моментом является постепенное налаживание взаимодействия между регулятором и финансовыми организациями в вопросах предотвращения и своевременного обнаружения киберинцидентов, а также минимизации их последствий. Все это позволяет надеяться на то, что в будущем удастся успешно противостоять росту масштабов компьютерной преступности в кредитно-финансовой сфере.

## Список литературы

APT-атаки на кредитно-финансовую сферу в России: обзор тактик и техник // Positive Technologies. – 2019. – 10.10. – URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/APT-Attacks-Finance-2019-rus.pdf (дата обращения 15.04.2020).

Банки демонстрируют киберхалатность // Газета РБК. – 2019. – 19.02, № 012 (2967). – URL: https://www.rbc.ru/newspaper/2019/02/19/5c6ac5439a794715806d3d6b (дата обращения 15.04.2020).

Банк России расширил требования по защите информации для кредитных организаций. – URL: https://www.cbr.ru/Press/event/?id=2630 (дата обращения 15.04.2020).

*Борисова Е.С., Белоусов А.Л.* Инновации как инструмент обеспечения информационной безопасности и повышения эффективности деятельности банковской системы // Актуальные проблемы экономики и права. – 2019. – Т. 13, № 3. – С. 1330–1342. – URL: https://cyberleninka.ru/article/n/innovatsii-kak-instrument-obespecheniya-informatsionnoi-bezopasnosti-i-povysheniya-effektivnosti-deyatelnosti-bankovskoi-sistemy (дата обращения 15.04.2020).

Защищенность кредитно-финансовой сферы, итоги 2018 года. Оценка Positive Technologies // Positive Technologies. – 2019. – 05.07. – URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Credit-and-Financial-Security-2019-rus.pdf (дата обращения 15.04.2020).

Кибератаки на банки: Тренды, уязвимости и роль регулятора. – 2018. – 27.07. – URL: https://www.plusworld.ru/professionals/kiberataki-na-banki-trendy-uyazvimosti-i-rol-regulyatora/ (дата обращения: 18.03.2019).

Обзор операций, совершенных без согласия клиентов финансовых организаций за 2019 год / Банк России, ФинЦЕРТ. – 2020. – 23 с. – URL: https://www.cbr.ru/Content/Document/File/103609/Review_of_transactions_2019.pdf (дата обращения 15.04.2020).

Обзор основных типов компьютерных атак в кредитно-финансовой сфере в 2018 году. – М.: Центральный банк РФ, 2019. – 88 с. – URL: http://www.cbr.ru/content/document/file/72724/dib_2018_20190704.pdf (дата обращения 15.04.2020).

Обзор основных типов компьютерных атак в кредитно-финансовой сфере в 2018 году / Банк России, ФинЦЕРТ. – 2019. – 86 с.

Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2019–2021 годов / Банк России. – 2019. – 24 с. – URL: https://www.cbr.ru/Content/Document/File/83253/onrib_2021.pdf (дата обращения 15.04.2020)

Основные направления развития финансовых технологий на период 2018–2020 годов / Банк России. – 2018. – 22 с. – URL: http://www.cbr.ru/content/document/file/85540/on_fintex_2017.pdf (дата обращения 15.04.2020).

Основные направления развития информационной безопасности кредитно-финансовой сферы на период 2019–2021 годов. – М.: ЦБ РФ, 2019. – 26 с.

Оценка влияния финансовых технологий на банковскую деятельность в России // Наука, технологии, инновации: Экспресс информация. – М.: ВШЭ, 2019. – 28.03. – URL: https://issek.hse.ru/data/2019/03/28/1187124654/NTI_N_125_28032019.pdf (дата обращения 15.04.2020).

*Перцева С.Ю.* Финтех-индустрия и информационная безопасность // Мировое и национальное хозяйство. – 2018. – № 4(46). – URL: https://mirec.mgimo.ru/upload/ckeditor/files/fintech-industry-and-information-society.pdf (дата обращения 15.04.2020).

ЦБ выявил в банках более 700 нарушений в сфере защиты информации. – 2019. – 06.11. – URL: https://www.plusworld.ru/daily/cat-security-and-id/tsb-vyyavil-v-bankah-bolee-700-narushenij-v-sfere-zashhity-informatsii/ (дата обращения 15.04.2020).

ЦБ обнаружил нарушения кибербезопасности во всех проверенных банках // РБК. – 2019. – 21.06. – URL: https://www.rbc.ru/finances/21/06/2019/5d0cc0189a7947b221a9492d (дата обращения 15.04.2020).

Future cyber threats: 2019 extreme but plausible threat scenarios in financial services // Accenture. – 2019. – URL: https://www.accenture.com/_acnmedia/pdf-100/accenture_fs_threat-report_approved.pdf (дата обращения 15.04.2020).

Group-IB: более 70% банков не готовы противостоять кибератакам // Group-IB. – 2019. – 19.02. – URL: https://www.group-ib.ru/media/banks-readiness/ (дата обращения 15.04.2020).

Hi-Tech Crime Trends 2018. Отчет о тенденциях высокотехнологичных преступлений // Group-IB. – 2018. – URL: https://www.group-ib.ru/resources/threat-research/2018-report.html (дата обращения 15.04.2020).

Hi-Tech Crime Trends 2019/2020 // Group-IB.–2019. – URL: https://www.group-ib.ru/resources/threat-research/2019-report.html (дата обращения 15.04.2020).

ICC 2019: Международный конгресс по кибербезопасности. – М., 2019. – URL: https://icc.moscow/upload/doc/ICC_reports_RU.pdf (дата обращения 15.04.2020).

Incident Response: Итоги года // Лаборатория компьютерной криминалистики Group-IB. – 2019. – 19.02. – URL: https://www.group-ib.ru/blog/incident (дата обращения 15.04.2020).

Lagarde Chr. Estimating cyber risk for the financial sector // IMFBlog: Insights & analysis on economics & finance. – 2018. – June 22. – URL: https://blogs.imf.org/2018/06/22/estimating-cyber-risk-for-the-financial-sector/ (дата обращения 15.04.2020).

The cost of cybercrime: Ninth annual cost of cybercrime study // Accenture. – 2019. – 23 p. – URL: https://www. accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom= (дата обращения 15.04.2020).

# ОНТОЛОГИИ И ПРОЕКТЫ ЭЛЕКТРОННЫХ ЗАКУПОК ЕВРОПЫ


**Куприяновский Василий Павлович**

Заместитель директора Центра цифровых высокоскоростных транспортных систем РУТ (МИИТ), заместитель директора центра геопространственного анализа экономического факультета МГУ (Москва, Россия)



**Климов Александр Алексеевич**

Кандидат технических наук, ректор Российского университета транспорта РУТ (МИИТ), (Москва, Россия)



**Покусаев Олег Николаевич**

Кандидат технических наук, директор Центра цифровых высокоскоростных транспортных систем Российского университета транспорта РУТ (МИИТ), (Москва, Россия)



***Аннотация.*** *В современных условиях финансирование сектора инновационных разработок, а также реализация масштабных инновационных проектов невозможны без участия государства. Одним из наиболее эффективных инструментов государственной поддержки являются государственные закупки. Настоящая статья посвящена анализу опыта ЕС по использованию современных цифровых технологий, включая область государственных закупок.*



***Ключевые слова:*** *цифровизация; цифровая экономика; информационное моделирование зданий; государственные электронные закупки.*

**Для цитирования:** Куприяновский В.П., Климов А.А., Покусаев О.Н. Онтологии и проекты электронных закупок Европы // Социальные новации и социальные науки. – Москва: ИНИОН РАН, 2020. – № 1. – С. 97–106.

URL: https://sns-journal.ru/ DOI: 10.31249/snsn/2020.01.07

## Введение

Цифровая экономика трансформирует очень многие процессы, протекающие в современном мире, заставляя его меняться. Государства переводят свои функции в цифровую среду, постепенно становясь «цифровыми» [Стратегический подход …, 2017; Принятие решений ..., 2017]. Однако цифровизация сама по себе не дает никакого экономического эффекта, а в худшем случае может приносить убытки, поглощая все большую часть государственных бюджетов. Так, государственные тендеры на разработку программных продуктов или реализацию сложных высокотехнологичных проектов, проведенные без привлечения специалистов, могут привести к неэффективному расходованию бюджетных средств. Анализ и распространение знаний о том, как эффективно перевести конкретный вид деятельности человека (экономической, управленческой и т.п.) в цифровую среду, как выглядят новые стандарты этой среды и как экономически выгодно работать в цифровом пространстве, связанном новыми отношениями с физическим миром, – представляет собой важную и актуальную задачу [Экономика стандартизации ..., 2016].

Необходимо отметить, что инновации происходят не только в цифровой сфере, но и в иных областях. Соединяясь, цифровые и нецифровые инновации изменяют ландшафт экономики [Информационные технологии ..., 2016].

Сегодня государству необходимо не просто стать «цифровым», но и научиться эффективно использовать финансовые ресурсы, чтобы обеспечить за счет инноваций стабильное и устойчивое развитие. Достичь этого можно разными способами. Наиболее важным инструментом являются государственные закупки разных уровней, которые составляют значительную часть ВВП. В настоящее время в данной области наибольшего успеха добились Европейский союз и отдельные страны Европы. И их опыт заслуживает внимательного изучения.

## Как из политики закупок технологий BIM возникла цифровая экономика

В Европе одним из предвестников цифровой экономики было внедрение правительством Великобритании технологий информационного моделирования зданий (BIM[1]) [Куприяновский, Синягов, Добрынин, 2016; Новая пятилетка BIM ..., 2016]. После кризиса 2008 г. правительство этой страны приняло решение развивать области, в которых можно достичь максимального экономического эффекта как на внутреннем рынке, так и в плане роста экспортного потенциала. Таким направлением стали тогда еще не очень известные технологии BIM. При этом основной упор был сделан на стандартизацию и организацию управления процессом. Главным же инструментом раз-

[1] BIM – англ. Building Information Model; в Градостроительном кодексе РФ – информационное моделирование.

вития данного направления стали государственные закупки центрального правительства, а также органов власти Англии, Шотландии, Уэльса и Северной Ирландии, составлявшие порядка 30% рынка. Политика «мягких посадок»[1] смягчала естественное сопротивление весьма косной строительной среды.

Довольно быстро проводимая политика дала видимые результаты, такие как сокращение сроков и снижение стоимости строительства, повышение уровня экологичности новых зданий, а также рост экспортного потенциала страны [Куприяновский, Синягов, Добрынин, 2016; Новая пятилетка BIM ..., 2016]. Следующим шагом стало использование технологии BIM для оптимизации цепочки поставок и основы для перехода промышленности к Индустрии 4.0 [The Future …, 2016].

Вторым следствием успешного использования технологии BIM в строительстве стало постепенное внедрение на практике идеологии «умного города». Таким образом, правительство Великобритании «запустило» переход к «цифровой экономике» [Куприяновский, Синягов, Добрынин, 2016].

Подчеркнем, что в основе успеха Великобритании в построении цифровой экономики и создании «умных городов» лежит экономическая заинтересованность бизнеса страны в соблюдении установленных государством стандартов и требований, поскольку это открывает ему доступ к государственным закупкам. Например, в Северной Ирландии все государственные закупки осуществляет Министерство финансов, которое в 2019 г. опубликовало уже третью версию руководства по закупкам BIM, включающую требования стандарта ISO 19650, что обеспечивает трансфер информации по всем стадиям жизненного цикла зданий и сооружений [Экономика стандартизации ..., 2016].

Успешная реализации в Великобритании технологии BIM сделала ее достаточно востребованной как для внедрения на этой базе различных инноваций, так и для использования в строительных проектах по всему миру. В качестве примера можно привести один масштабный проект, реализуемый в Китае, – строительство (в рамках подготовки к проведению зимних Олимпийских игр 2022 г.) скоростной железной дороги Пекин – Чжанцзякоу (протяженностью 174 км и с расчетной скоростью движения 350 км/час). «Новая скоростная линия, включающая 71 наземный участок, 64 моста, 10 тоннелей и 10 станций, в том числе самую глубокую и самую большую в мире станцию метро в Бадалине, стала первой в Китае, где внедрена стратегия BIM с полным жизненным циклом» [Illankoon …, 2020]. Особенностью этого проекта является еще и то, что в нем предусматривается создание «цифровых двойников»[2]. Можно представить также сложность за-

[1] Политика мягких посадок – от английского Soft Landing – комплекс мер государственной поддержки стартапов и стимулирования бизнеса к внедрению новых технологий.

[2] Цифровой двойник (англ. Digital Twin) – цифровая копия физического объекта или процесса, помогающая оптимизировать эффективность бизнеса. Концепция «цифрового двойника» является частью четвертой промышленной революции и призвана помочь предприятиям быстрее обнаруживать физические проблемы, точнее предсказывать их результаты и производить более качественные продукты.

купки строительных услуг по созданию того, чего еще никогда в мире не существовало, причем в очень жесткие сроки [Цифровые двойники ..., 2020].

## Основная онтология электронных закупок Европейского союза

В Европейском союзе государственные закупки затрагивают практически каждую организацию. Расходы самого ЕС и входящих в него стран скоро превысят 2 трлн евро в год, причем государственные закупки в сфере строительства, включая закупки технологии BIM, составляют существенную их часть. Очевидно, что в современных сложных экономических условиях существует настоятельная необходимость в наиболее эффективном управлении государственными финансами. Нельзя забывать, что закупочная деятельность в каждой стране ЕС имеет свои особенности. Построение в таких условиях экономически выгодной системы закупок является очень сложной задачей даже с привлечением формальных онтологий[1] и новых цифровых технологий.

Связь цифровой экономики с формализованными онтологиями, решения по онтологиям закупок, опыт их применения в ЕС детально анализировались в ряде работ отечественных экспертов [Проблемы цифровой экономики ..., 2018; К вопросу об эффектах ..., 2018; Онтологизация данных ..., 2018; К вопросу обратного инжиниринга ..., 2019]. Отмечается, что в условиях возрастающего значения стандартов данных для электронных закупок в последние годы был запущен ряд инициатив по их созданию, которые реализовались государственным сектором, частными компаниями и научными кругами. Словари и семантика, которую они вводили, фазы государственных закупок, которые они охватывали, и технологии, которые они использовали, сильно различались между собой. Эти различия затрудняли совместимость данных и их повторное использование, что обусловило необходимость общего представления знаний в области электронных закупок для ЕС.

В 2016 г. Бюро публикаций ЕС (Publications Office) было поручено организовать и поддержать разработку Онтологии государственных электронных закупок (ePO), которая позже стала международным стандартом для закупок BIM. Цель онтологии – концептуализировать, формально кодировать и предоставлять в открытом, структурированном и машиночитаемом формате данные о государственных закупках, включая все этапы от размещения информации о предстоящем тендере и до момента оплаты. Для этого нужен общий словарный запас, аксиомы и правила. Первая версия Онтологии была опубликована в середине 2017 г., а вторая – в январе 2018 г. Важным моментом в разработке ePO было то, что она опиралась на мнение ключевых мировых экспертов, а не чиновников, что соответствует общемировым трендам. Благодаря общности подхода достаточ-

[1] Понятие онтологий или формальных (машинно-интерпретируемых) формулировок терминов предметной области и отношений между ними пришло из лабораторий по искусственному интеллекту и в настоящее время широко распространилось среди экспертов в других областях научного знания, которые используют его в качестве синонима понятиям «принципы» (основные подходы или положения) и «свод» (словарь, библиотека) правил. – *Прим. ред.*

но быстро решались вопросы совместимости и взаимного использования онтологических формализаций.

Сегодня Бюро публикаций ЕС (далее – Бюро) является главным органом цифрового правительства ЕС и отвечает за размещение в Интернете всех официальных данных, которые создают органы Союза и государств-членов. В частности, Бюро управляет целым рядом веб-сайтов, предоставляющих гражданам ЕС, правительствам и предприятиям цифровой доступ к таким базам, как EUR-Lex (публикация законов и нормативных актов ЕС), портал открытых данных ЕС (включая ссылки на открытые данные стран – членов ЕС), информация о тендерах ЕС (TED – Tenders Electronic Daily). Бюро также предоставляет частному сектору возможности по созданию различных приложений и цифровых сервисов на базе размещаемых им данных. Кроме того, поскольку Бюро поддерживает коммуникации практически со всеми государственными органами Союза и его членов, у него открываются огромные возможности междоменного онтологического взаимодействия при проведении электронных закупок [Publications Office …].

В 2020 г. Бюро опубликовало отчет об электронных закупках в ЕС [Interoperability …, 2020]. Основной акцент в нем сделан на функциональную совместимость, т.е. «способность организаций взаимодействовать для достижения взаимовыгодных целей, включая обмен информацией и знаниями между этими организациями через поддерживаемые ими бизнес-процессы посредством обмена данными между их системами ИКТ» [Interoperability …, 2020]. При этом совместимость электронных закупок тесно связана с функциональной совместимостью в более широком контексте цифрового правительства.

Функциональная совместимость между системами электронных закупок улучшает соотношение цены и качества при государственных закупках. Это достигается за счет усиления конкуренции (в основном благодаря лучшим решениям) и более качественных данных. Заказчики также выигрывают от повышения качества данных и облегчения процедур, что обеспечивает большую эффективность процесса закупок. Кроме того, растет конкурентоспособность компаний, поскольку вместо того, чтобы тратить ресурсы на административные требования, они должны улучшать свое предложение. Наконец, увеличивается общая прозрачность государственных закупок.

Взаимодействие (совместимость) должно быть достигнуто на четырех уровнях – юридическом, организационном, семантическом (в том числе синтаксическом) и техническом – и поддерживаться хорошим управлением. В сфере электронных закупок больше всего усилий требуется приложить на семантическом и организационном уровнях. Основными проблемами здесь являются нечеткое управление, разная зрелость платформ и неопределенное восприятие [Interoperability …, 2020].

## Другие онтологии и проекты ЕС в области электронных закупок

Помимо Онтологии электронных закупок ЕС – центрального звена развивающейся системы электронных закупок Союза, – в регионе реализуются и другие проекты в этой области. Основываясь на материале [Interoperability …, 2020], можно дать их следующую краткую характеристику.

Уже сегодня для всех заказчиков в ЕС обязательны единые стандартные формы. Благодаря этому компаниям стало легче находить объявления о тендерах. Для граждан информация о закупках также стала более прозрачной, а правительствам это позволяет принимать обоснованные решения о расходах бюджетов. Стандартные формы TED важны для функциональной совместимости, поскольку они обобщают информацию на большинстве этапов закупок: планирование, объявление о тендере, его проведение, заключение контракта и его исполнение.

Директива ЕС об электронных счетах при государственных закупках направлена на облегчение их использования операторами при поставках товаров, работ и услуг для государственного сектора. Директива обязывает организации-заказчики получать и обрабатывать электронные счета в соответствии с европейским стандартом, разработанным Техническим комитетом CEN 434 [Interoperability …, 2020].

Директива о государственных закупках 2014/24/EU утвердила Европейский единый документ о закупках (ESPD), который определяет единые критерии отбора поставщиков. С апреля 2018 г. ESPD используется в электронном виде в двух стандартных формах: базовой (которая соответствует только минимальным требованиям Регламента) и расширенной (которая может полностью заменить всю информацию о критериях отбора поставщика и об основаниях исключения участников тендера). Если документы, подтверждающие соответствие участника государственных закупок установленным требованиям, уже размещены на едином портале государственных закупок, то другой информации не требуется. Хотя это обязательство можно выполнить вручную, созданная онлайн-база данных позволяет осуществлять автоматический обмен структурированными данными. В системе перечислены критерии приемлемости и документальные подтверждения, необходимые в каждой стране ЕС для участия в государственных закупках. Это помогает участнику тендера определить, какие документы и сертификаты необходимо представить; заказчику – какие документы они могут найти в базе, а какие необходимо дополнительно запросить у будущих подрядчиков. Наконец, всем участникам торгов это помогает определить, какие сертификаты имеют одинаковую юридическую силу в разных странах.

Европейской комиссией в качестве одного из первых стандартов консорциума европейских заказчиков был определен Универсальный бизнес-язык (UBL), и он теперь доступен для всех без каких-либо лицензионных сборов. UBL является результатом международных усилий по созданию бесплатной библиотеки стандартных электронных бизнес-документов XML, таких как заказы

на покупку и счета. Он предназначен для использования в существующих юридических, деловых, аудиторских и управленческих практиках, устраняя необходимость повторного ввода в существующие цепочки поставок факсимильных и бумажных документов. Он уже применяется разными странами для трансграничных транзакций, связанных с поставками, закупками (например, электронное выставление счетов) и транспортировкой (например, накладные). Стандарт является основой для нескольких европейских систем государственных закупок, включая EHF (Норвегия), Svekatalog, Sveorder и Svefaktura (Швеция), OIOUBL (Дания), e-Prior (Европейская комиссия DIGIT) и PEPPOL (Панъевропейский проект государственных закупок в режиме онлайн).

PEPPOL был инициирован в 2008 г. и призван облегчить проведение трансграничных электронных закупок. Он предоставляет собой набор технических спецификаций, которые могут быть реализованы в существующих решениях для электронных закупок, чтобы сделать их совместимыми. Устойчивость проекта PEPPOL обеспечивается Ассоциацией OpenPEPPOL, созданной в 2012 г.

В 2017 г. завершился проект e-SENS – разработка пилотной программы электронных закупок с техническими решениями для следующих случаев:

– электронные торги: компаниям предоставляется возможность подать заявку на тендер, проводимый в любом государстве – члене ЕС, и получить ответ от компетентного органа благодаря бесперебойной связи между системами всех государств;

– виртуальное досье компании: формирование электронного информационного пакета, включающего все необходимые для участия компании в торгах документы;

– электронное выставление счетов.

После завершения проекта все спецификации e-SENS были переданы для внедрения OpenPEPPOL.

В 2017 г. был запущен и действует по настоящее время Проект принципа «единожды» (TOOP). Суть его заключается в том, чтобы компаниям не требовалось каждый раз предоставлять одни и те же документы для участия в тендере. Теперь все они хранятся в специальных реестрах, и система находит их автоматически в случае необходимости.

В рамках Программы ЕС по решениям для обеспечения взаимодействия (ISA) международными рабочими группами был создан ряд основных словарей, призванных содействовать обмену информацией между органами власти и решению проблем совместимости. Основные словари – это упрощенные, многократно используемые и расширяемые модели данных, которые отражают фундаментальные характеристики объекта в независимом от контекста виде. В настоящее время доступны следующие словари:

– основной словарь человека: фиксирует основные характеристики человека, например, имя, пол, дата рождения, место жительства;

– основной словарь государственной службы: отражает основные характеристики услуг, предлагаемых органами власти;

– основной деловой словарь: фиксирует основные характеристики юридического лица (например, его идентификатор, виды деятельности) и создается посредством формального процесса регистрации, обычно в национальном или региональном реестре;

– основной словарь общественной организации: фиксирует основные характеристики общественных организаций в ЕС;

– основной словарь местоположения: фиксирует основные характеристики местоположения в виде адреса и географического названия;

– словарь основных критериев и доказательств: описывает требования, которые частное лицо должно соблюсти, чтобы получить государственную услугу.

В сфере закупочной деятельности эти словари особенно актуальны, поскольку в них описываются основные стороны и элементы государственных контрактов. Кроме того, словарь базового местоположения может предоставить решение для описания любых необходимых данных расположения заказчика и поставщика.

Институтом носителей знаний Открытого университета (Великобритания) разработана онтология для представления европейских уведомлений о государственных закупках – Связанные открытые тендеры Electronic Daily (LOTED). Модель LOTED2, с одной стороны, содержит нормативную базу закупочной деятельности, а с другой – сохраняет удобство использования, необходимое для семантических приложений.

В 2010 г. Органом по стандартизации местного электронного правительства и Группой местного самоуправления в рамках инициативы правительства Великобритании по обеспечению прозрачности была создана Онтология платежей – словарь общего назначения для публикации данных об организационных расходах в виде таблицы.

Партнерством открытого контракта (OCP) был разработан Открытый стандарт данных о контрактах (OCDS), который позволяет раскрывать данные и документы на всех этапах процесса заключения контрактов благодаря общей модели данных. Он был создан с целью повышения прозрачности государственных закупок и более глубокого анализа контрактов широким кругом пользователей.

При разработке технических спецификаций электронных закупок используется Европейская эталонная архитектура взаимодействия (EIRA), которая является частью Программы ЕС по решениям для обеспечения взаимодействия (ISA2). EIRA определяет наиболее важные архитектурные блоки, необходимые для создания совместимых систем электронного правительства. Она также

предоставляет общую терминологию, которая может использоваться государственными органами при решении различных задач и разработке разных систем.

Проект SPICE («умные закупки для лучшего транспорта») призван помогать государственным органам использовать лучшие практики и рекомендации. Он собирает и анализирует практику государственных закупок для проектов по устойчивому транспорту и мобильности в Европе и представляет передовой опыт государственным заказчикам. Кроме того, используя платформенный принцип, SPICE может формировать ряд общих групп заказчиков в целях планирования совместных трансграничных закупочных мероприятий для транспортных проектов.

Проект TheyBuyForYou работает над принципиально важной для электронных закупок темой – сбором данных о цепочках создания стоимости, управлении спросом, конкурентных рынках и аналитики для поставщиков.

## Заключение

Европейская комиссия оценивает сумму закупок, осуществляемых в соответствии с директивами ЕС, более чем в 500 млрд евро, или приблизительно 4% ВВП Союза [Interoperability …, 2020]. Следовательно, любые меры, направленные на упрощение системы закупок и снижение административных барьеров для поставщиков, ведут к значительным выгодам для всех участвующих сторон.

Удивительные по последствиям эффекты можно ожидать, когда электронная система закупок ЕС станет использовать Интернет вещей, запуск которого в Европе ожидается уже к 2030 г. [На пути к физическому интернету …, 2019].

Вместе с тем отмечается ряд проблем развития электронных закупок в ЕС, значительная часть которых, как мы полагаем, свойственна и России, в том числе следующие [Interoperability …, 2020]:

– конкуренция в сфере государственных закупок, как и участие в них частных компаний, остается низкой и имеет тенденцию к снижению;

– в настоящее время не существует единого рынка решений для электронных закупок. Вероятно, это связано с проблемами совместимости различных электронных площадок и ресурсов, но также является наиболее частой причиной отказа компаний от участия в закупках;

– компании не имеют достаточной информации о закупочных процедурах.

Очевидно, что развитие системы электронных закупок связано с дополнительными инвестициями в разработку и внедрением цифровых технологий, направленных на повышение совместимости электронных ресурсов в данной области и распространение нормативной информации.

Цифровизация государственных закупок позволяет более эффективно расходовать государственные средства. Одновременно повышается степень прозрачности процедур, что, в свою оче-

редь, снижает уровень коррупции, способствует расширению круга участников торгов и росту доверия к государственным институтам.

## Список литературы

Информационные технологии в системе университетов, науки и инноваций в цифровой экономике на примере Великобритании / Куприяновский В.П., Синягов С.А., Намиот Д.Е., Добрынин А.П., Черных К.Ю. // International Journal of Open Information Technologies. – 2016. – Vol. 4, N 4. – С. 30–39.

К вопросу об эффектах применения формализованных онтологий в экономике данных – опыт ЕС / Куприяновский В.П., Волокитин Ю.И., Понкин И.В., Синягов С.А., Намиот Д.Е., Добрынин А.П. // International Journal of Open Information Technologies. – 2018. – Vol. 6, N 8. – С. 66–78.

К вопросу обратного инжиниринга – путь от бумаги до цифровых онтологических правил для образовательных технологий / Климов А.А., Куприяновский В.П., Гринько О.В., Покусаев О.Н. // International Journal of Open Information Technologies. – 2019. – Vol. 7, N 9. – С. 82–91.

*Куприяновский В.П., Синягов С.А., Добрынин А.П.* BIM – Цифровая экономика. Как достигли успеха? Практический подход к теоретической концепции // International Journal of Open Information Technologies. – 2016. – Vol. 4, N 3. – С. 1–20.

На пути к физическому интернету: индустрия, логистика и электронная коммерция 4.0. Европейский вариант / Куприяновский В.П., Климов А.А., Покусаев О.Н., Намиот Д.Е., Катцын Д.В. // International Journal of Open Information Technologies. – 2019. – Vol. 7, N 5. – С. 89–104.

Новая пятилетка BIM – инфраструктура и умные города / Куприяновский В.П., Синягов С.А., Намиот Д.Е., Бубунов П.М., Куприяновская Ю.В. // International Journal of Open Information Technologies. – 2016. – Vol. 4, N 8. – С. 20–35.

Онтологизация данных Европейского союза как переход от экономики данных к экономике знаний / Гринько О.В., Куприяновский В.П., Покусаев О.Н. и др. // International Journal of Open Information Technologies. – 2018. – Vol. 6, N 11. – С. 65–84.

Принятие решений в цифровой экономике. Опыт Великобритании / Куприяновский В.П., Евтушенко С.Н., Дунаев О.Н., Дрожжинов В.И., Намиот Д.Е. // International Journal of Open Information Technologies. – 2017. – Vol. 5, N 4. – С. 63–73.

Проблемы цифровой экономики и формализованные онтологии / Волокитин Ю.И., Куприяновский В.П., Гринько О.В., Покусаев О.Н., Синягов С.А. // International Journal of Open Information Technologies. – 2018. – Vol. 6, N 6. – С. 87–96.

Стратегический подход к формированию цифрового правительства США / Дрожжинов В.И., Куприяновский И.П., Евтушенко С.Н., Намиот Д.Е. // International Journal of Open Information Technologies. – 2017. – Vol. 5, N 4. – С. 29–54.

Цифровые двойники на базе развития технологий BIM, связанные онтологиями, 5G, IoT и смешанной реальностью для использования в инфраструктурных проектах и IFRABIM / Куприяновский В.П., Климов А.А., Воропаев Ю.Н. и др. // International Journal of Open Information Technologies. – 2020. – Vol. 8, N 3. – С. 55–74.

Экономика стандартизации в цифровую эпоху и информационно-телекоммуникационные технологии на примере Британского института стандартов / Куприяновский В.П., Ярцев Д.И., Уткин Н.А., Намиот Д.Е. // International Journal of Open Information Technologies. – 2016. – Vol. 4, N 6. – С. 1–9.

ePO – eProcurement Ontology 2.0.0 [Report] // Publications Office of the EU. – 2018. – URL: https://eprocurement-everis.github.io/ (дата обращения 10.03.2020).

European Union Location Framework – Guidelines for public procurement of geospatial technologies // The European Commission's science and knowledge service. – 2016. – URL: https://ec.europa.eu/jrc/en/publication/european-union-location-framework-guidelines-public-procurement-geospatial-technologies (дата обращения 12.03.2020).

Government Soft Landings Revised guidance for the public sector on applying BS8536 parts 1 and 2 // Centre for Digital Built Britain. – 2019. – URL: https://ukbimframework.org/wp-content/uploads/2019/11/GSL_Report_PrintVersion.pdf (дата обращения 11.03.2020).

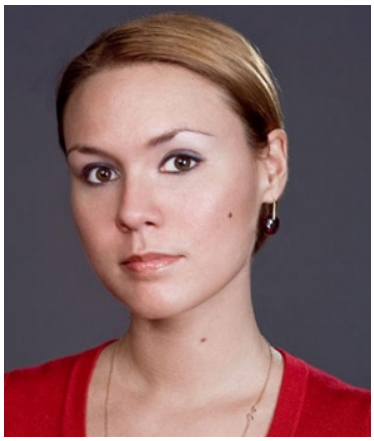
Illankoon K. China Railway Sets Benchmark for Full-lifecycle BIM on Beijing-Zhangjiakou Rail Project // Construction Business News. – 2020. – 23.03. –URL: https://www.cbnme.com/logistics-news/china-railway-sets-benchmark-for-full-lifecycle-bim-on-beijing-zhangjiakou-rail-project/ (дата обращения 12.03.2020).

Interoperability in end-to-end eProcurement // Publications Office of the EU. – 2020. – 10.02. – URL: https://op.europa.eu/en/publication-detail/-/publication/1c578b32–4c82–11ea-b8b7–01aa75ed71a1/language-en (дата обращения 11.03.2020).

Publications Office of the EU. – URL: https://op.europa.eu/en/web/about-us/who-we-are (дата обращения 11.03.2020).

The Future for Construction Product Manufacturing Digitalisation, Industry 4.0 and the Circular Economy // Construction Products Association UK. – 2016. – 62 с. – URL: http://thenorrisgroup.com/learning/files/media_manager/original/106.pdf (дата обращения 12.03.2020).

# МЕНТАЛЬНАЯ БЕЗОПАСНОСТЬ В ЭПОХУ ЦИФРОВИЗАЦИИ




**Коровникова Наталья Александровна**

Кандидат политических наук, старший научный сотрудник Отдела экономики, Институт научной информации по общественным наукам РАН (ИНИОН РАН), (Москва, Россия)



***Аннотация.*** *В статье раскрываются представления о ментальном пространстве, а также угрозы его функционированию и развитию в условиях цифровизации. Показано взаимодействие ментального и образовательного пространств. Описана взаимосвязь ментальной, образовательной и национальной безопасности в контексте перехода в цифровую эпоху.*



***Ключевые слова:*** *ментальное пространство; образовательное пространство; безопасность; цифровизация.*

**Для цитирования:** Коровникова Н.А. Ментальная безопасность в эпоху цифровизации // Социальные новации и социальные науки. – Москва: ИНИОН РАН, 2020. – № 1. – С. 107–118.

URL: https://sns-journal.ru/ DOI: 10.31249/snsn/2020.01.08

## Введение

На современном этапе глобальной эволюции цифровизация представляет собой один из основных трендов мирового развития. Повсеместный характер цифровизации объясняет не только существенные модификации материально-производственной сферы, обусловленные переходом к цифровой экономике, но и значительные трансформации «в сфере когнитивных процессов, к которым обычно относят память, внимание, восприятие, понимание, мышление, процессы принятия решений» [Современная когнитология, 2014, с. 133].

Переход в цифровую эру предполагает постоянную и своевременную адаптацию к динамичному изменению среды на всех уровнях: личностном, групповом, национальном и глобальном. В связи с этим качество человеческого капитала и его интеллектуальная составляющая, которые являются непосредственным результатом образовательных процессов, становятся важнейшими факторами как экономического роста, так и национальной безопасности. В связи с этим требуется более детальное изучение рисков и перспектив цифровизации с точки зрения обеспечения безопасности ментального пространства (ментальной безопасности), которая представляется актуальным объектом междисциплинарных исследований.

## Ментальное пространство: понятия, особенности, риски

На сегодняшний день в экспертной среде не сложилось единого подхода к определению смежных понятий «менталитет», «ментальность», «ментальное пространство» – их значение часто обусловлено ракурсом конкретного исследовательского проекта.

В широком смысле «менталитет» – это «образ мысли, совокупность умственных навыков, духовных установок и культурных традиций, присущих отдельному человеку и человеческой общности» [Богданова, 2015]. Его рассматривают как «фундаментальный слой коллективного поведения, деятельности, эмоционального реагирования на различные ситуации, присущие данному этносу или устойчивой социальной группе» [Дзялошинский, 1996], который формируется «в подсознании, но постоянно впитывает в себя то общее, что складывается из природных данных и социально обусловленных элементов и в конечном итоге выражается в представлении о жизни и окружающем мире», а также «отражает устойчивые привычки, нравы и формы поведения» социума [Богданова, 2015]. Выделяют следующие уровни (разновидности) менталитета: «индивидуальный»; «космоцентрический» или теократический («все сущее» – творение Бога); «социоцентрический» («растворение» личности в «Мы»-общности); «эгоцентрический» (стремление к власти) [Дзялошинский, 1996].

Понятие «ментальность» подразумевает «способ видения мира, сформированный в процессе воспитания, образования и обретения жизненного опыта в конкретной культурной среде» [Сидоров, 2015, с. 85], который аккумулирует «морально-нравственные ценности, набор психологических и поведенческих реакций, особенности адаптации» [Что такое ментальность, 2019]. Данное понятие включает в себя «константы» жизненных установок, моделей поведения, эмоций и настроений», «опирается на глубинные зоны, присущие данному обществу и культурной традиции» [Дзялошинский, 1996]. Ментальность как многоаспектный феномен, который охватывает сферы сознательного и бессознательного, логического и эмоционального, представляет собой источник мышления, веры, чувств и эмоций, детерминированный конкретными историческими условиями жизнедеятельности социума, в настоящих условиях – особенностями цифровых трансформаций.

В научный оборот (первоначально в когнитивную лингвистику) термин «ментальное пространство», как «постоянно модифицируемый когнитивный конструкт», был введен Ж. Фоконье и М. Тернером в рамках теории концептуальной интеграции (англ. Blending Theory) и теории ментальных пространств (англ. Mental Space Theory) [Ирисханова]. В современном научном дискурсе понятие «ментальное пространство» стало применяться в разных областях, включая психологию мышления, психосемантику, психолингвистику, компьютерную лингвистику и инженерию знаний [Шамаев, 2002]. Особую популярность данный термин приобрел в 1980-е годы в связи с «лавинообразной компьютеризацией мира», способствовавшей формированию новой «образной организации» ментальных пространств человека, которые являются продуктом внутренней психической деятельности («умственно создаваемые построения»), имеют эмпирические характеристики различных образных ментальных репрезентаций, выполняют когнитивную функцию «временно сохранять релевантную для субъекта информацию, а также результаты ее преобразований в процессе понимания» [Осорина, 2017, с. 6–10].

Типы ментальных пространств, обусловленные особенностями их основ – менталитета и ментальности, – подразделяются на «ассоциативные» (связи «элемент – элемент»); «с ограничениями по типам связей» (антонимия, синонимия); «с более сложными ограничениями на классы элементов и типы связей»; «пространственно-временные» (соотношения, образующие континуум во времени и пространстве) [Шамаев, 2002]; а также классифицируются в зависимости от ступени развития общества, расовой принадлежности, гендерных признаков, возрастных характеристик, религиозных и / или идеологических убеждений, уровня интеллекта (образованности) [Что такое ментальность, 2019].

Перспективы дальнейшей (в том числе цифровой) эволюции ментальных пространств предполагают: применение пространственно-временного способа кодирования и организации когнитивного (ментального) материала; возможность использовать «величину ментального объекта как

показатель его значимости»; приватность образования и функционирования когнитивных структур [Осорина, 2017, с. 13–14]; снижение уровня аналитического мышления на фоне развития интуитивного и / или творческого мышления [Современная когнитология, 2014, с. 141].

В условиях цифровизации важную организующую роль в создании и управлении ментальными пространствами стали играть определенные технологические структуры, формирующие ментальный мир современного человека, например такие компании, как Apple, Google, Facebook, YouTube, Snapchat, Instagram и др. На сегодняшний день они обладают наиболее эффективными инструментами влияния на ментальность населения, более значимыми, чем религии и государственная власть [Почепцов, 2018].

Все субъекты современных ментальных пространств столкнулись с необходимостью цифровой трансформации, которая предполагает изменение моделей поведения и бизнеса на основе применения новых информационных и сетевых технологий [Вызовы цифровой экономики, 2019, с. 401–403]. Повсеместная компьютеризация и цифровизация значительной части ментального пространства на всех иерархических уровнях имеет целый ряд положительных эффектов: динамичность развития, рост качества жизни, совершенствование человеческого капитала, личностный и социальный прогресс и т.п. Однако имеют место и отрицательные последствия для эволюции ментальной сферы. Эксперты называют следующие:

– ментальные вирусы и эпидемии (психические и психосоматические расстройства и состояния индивидуального и общественного сознания)[1] [Сидоров, 2015, с. 85];

– рост количества и разновидностей ментальных расстройств, например: «синдром рассеянного внимания»; «синдром ментального иммунодефицита»; «синдром экзистенциальной безысходности»; «деструктивный социогенез» (растущая социальная деформация, усиление депривационно-изоляционных трендов, распространение псевдообщественных институтов); «деструктивный психогенез» (кризис индивидуальной и коллективной идентичности, деформация индивидуального и общественного сознания); «деструктивный анимогенез» (культуральная деформация, нарушение морально-нравственной социализации, деградация образовательных систем, маргинализация и унификация общественной жизни) [Современная когнитология, 2014, с. 134; Сидоров, 2015, с. 89–90];

– культурная гипертекстуальность (нелинейная, ассоциативная генерация идей), развивающаяся в результате непрерывно растущего объема информации, языковых трансформаций, виртуальной коммуникации, распространения «кнопочной культуры» и «киберязыка» («e-language»), а также повсеместной визуализации культуры [Современная когнитология, 2014, с. 134–136, 140];

[1] Исследование ментальных вирусов и эпидемий осуществляется в рамках нового научного направления – ментальной эпидемиологии, – изучающей различные угрозы (события, состояния и т.п.) ментальному здоровью личности и возможности «адаптивной защиты общественного ментального здоровья» [Сидоров., 2015, с. 85].

– формирование субкультур деструктивной направленности, прежде всего молодежных (например, феномен группы NEET, которую объединяет удовлетворение потребности в коммуникации исключительно в цифровом пространстве), псевдозанятости, отсутствия важных морально-нравственных качеств (трудолюбия, ответственности и др.), эгоистической потребительской идеологии, отрицания обязательности труда и т.п. [Ломоносовские чтения, 2019, с. 583];

– изменение направленности когнитивных процессов, переход от рационального мышления к «клиповому мышлению» (которое предполагает «процесс отражения множества разнообразных свойств объектов, без учета связей между ними», а также характеризуется фрагментарностью информационного потока, алогичностью и гетерогенностью воспринимаемой информации, высокой скоростью переключения между фрагментами информации, «отсутствием целостной картины восприятия окружающего мира») [Современная когнитология, 2014, с. 137–138];

– снижение словесно-логической памяти, выражающейся в восприятии метаинформации, т.е. информации о месте ее хранения в цифровом пространстве [Современная когнитология, 2014, с. 140];

– «утечка мозгов» и ментальных ресурсов в социальные сети, в результате которых широкое распространение получил психологический таргетинг[1], подразумевающий создание индивидуальных психологических портретов и использование личной информации пользователей [Почепцов, 2018];

– поляризация и фрагментация социума, которые выражаются в крайних формах индивидуализма, росте экономического неравенства, различных видах терроризма (в том числе ментально-информационных), дегуманизации социально-трудовых и экономических отношений [Ломоносовские чтения, 2019, с. 578; Золотухин М.А., 2018, с. 119] и нарастании депопуляционных трендов [Сидоров, 2015, с. 89];

– преобладание деструктивного использования сетей над деятельностью «киберполицейских» [Почепцов, 2018] в результате недостаточной правовой грамотности большинства пользователей, а также разобщенности лиц и организаций, обеспечивающих безопасность в цифровом и, как следствие, в ментальном пространстве.

## Образование как фактор формирования ментального пространства

Цифровизация существенно трансформирует традиционные хозяйственные отношения и бизнес-модели. В современных условиях основным фактором производства, социального развития и экономического роста становится кадровый потенциал с новыми информационно-сетевыми

[1] Таргетинг (от англ. target – цель) – рекламный механизм, позволяющий выделить целевую аудиторию и показать рекламу именно ей.

свойствами, функциями и компетенциями [Вызовы цифровой экономики, 2019, с. 373]. Важнейшим инструментом их генерирования является образование.

Цифровизация материально-производственного и ментального (когнитивно-аксиологического) пространства в целях формирования цифровой ментальности предполагает модификацию современного образования с внедрением новейших методов и инструментов (особенно в области высшего образования), при безусловном сохранении «глубины и фундаментальности» традиционных образовательных форм [Актуальные проблемы менеджмента, 2017, с. 50; Ломоносовские чтения, 2019, с. 526].

Сфера общественно-профессиональной деятельности, которая направлена на формирование индивидуальности, увеличение человеческого капитала, укрепление духовного, интеллектуального и экономического потенциала общества – другими словами, на непрерывное целенаправленное социокультурное воспроизводство ментального пространства индивида, социума и государства, – выступает в качестве образовательного пространства [Золотухин, 2018, с. 118]. Образовательное пространство включает знания, накопленные обществом; умения, навыки и компетенции населения; сеть образовательных учреждений, образовательную инфраструктуру; систему финансирования образовательной деятельности; регулирующие политико-правовые нормы.

Обеспечение соответствия развития образовательного пространства потребностям процесса цифровизации в современных условиях требует:

– формирования системы трудовых отношений, отвечающих реалиям цифровой эпохи, и их нормативно-правовое закрепление;

– создания вариативной аттестации компетенций согласно профессиональным и образовательным стандартам национальной и международной систем квалификаций;

– разработки базовых образовательных программ, обеспечивающих цифровую грамотность кадров;

– реализации стратегии непрерывного образования, в том числе механизмов переподготовки, повышения квалификации и вовлечения в цифровую экономику возрастных социальных групп (специалистов старше 50 лет, пенсионеров и инвалидов), а также государственных служащих и самих педагогических работников;

– создания эффективной системы мотивации участия населения в мероприятиях по переходу в цифровую эпоху [Актуальные проблемы менеджмента, 2017, с. 51];

– повышения влияния современного образования на процесс формирования менталитета независимо от профиля и уровня образовательного учреждения [Богданова, 2015];

– подготовки трудовых ресурсов в соответствии с тем, что наукоемкий труд становится основой экономического роста [Актуальные проблемы менеджмента, 2017, с. 53];

– выработки инновационных стратегий в области обучения персонала работе с новейшими технологиями «цифровых сервисов» [Актуальные проблемы менеджмента, 2017, с. 555–556].

В свою очередь, формирование и адаптация ментального пространства к новым «цифровым» условиям посредством образования предполагает решение следующих задач: 1) трансляции наиболее стабильных исторически сложившихся духовных, мировоззренческих и культурных ценностей в качестве нравственных ориентиров; 2) обогащения индивидуальных и общественных ментальных качеств конкретного социума нравственными общечеловеческими идеалами; 3) коррекции и преобразования «ментальной энергии» социума на достижение целей цифровизации [Богданова, 2015]; 4) последовательной разработки и внедрения конкурентоспособных образовательных цифровых инноваций; 5) создания и накопления готового к деятельности высококвалифицированного человеческого капитала [Актуальные проблемы менеджмента, 2017, с. 558–559].

Адекватная модификация современного образования подразумевает: рост затрат на образование на уровне личности, организации, государства, мира; усложнение структуры высшего образования (бакалавриат, магистратура, аспирантура, дополнительное образование); коммерциализацию части образовательных услуг; коммодитизацию (обезличивание) за счет обеспечения доступности учебных материалов с помощью цифровых технологий [Золотухин, 2018, с. 118]. Одновременно происходит формирование специфической культуры «неявного знания», которая повышает результативность прочих знаний, умений и навыков, и включает следующие составляющие: а) культуру работы с данными; б) культуру работы с научной и иными видами информации; в) культуру использования количественных методов; г) культуру сочетания традиционных методов проверки гипотез с новыми методами и принципами обработки данных [Ломоносовские чтения, 2019, с. 527].

Цифровые трансформации образовательного пространства, непосредственно влияющие на изменения в ментальной сфере социума, предполагают адаптацию нормативно-правового обеспечения образовательных процессов к условиям цифровизации; готовность учебных заведений к внедрению и использованию новых образовательных технологий; создание благоприятных организационных и экономических условий для развития новых направлений и программ подготовки востребованных кадров [Ломоносовские чтения, 2019, с. 487, 580].

К числу новейших образовательных инструментов и методов цифровой эпохи относятся [Ломоносовские чтения, 2019, с. 487, 506–507]:

– онлайн-коучинг[1], который при минимальных требованиях к программному и аппаратному обеспечению становится широко и повсеместно доступным;

[1] Метод консалтинга и тренинга (англ. coaching), в процессе которого человек, называющийся «коуч» (личный тренер), помогает обучающемуся достичь некой жизненной или профессиональной цели.

– образовательные интернет-платформы, представляющие новейшие направления (цифровая журналистика и т.п.) и учебные курсы от ведущих вузов (наиболее известные российские платформы – «Открытое образование» и «Универсариум»);

– облачные технологии хранения и обработки данных, позволяющие при низких технологических затратах и простоте использования стимулировать взаимодействия субъектов образовательного пространства;

– концепция BYOD («Принеси свое собственное устройство»), в рамках которой обучаемый сам управляет учебным процессом (определяет темп обучения, оценивает прогресс и т.п.) при условии адаптации образовательных продуктов под личные гаджеты;

– машинное обучение, которое персонализирует образовательный процесс, позволяет применять большие массивы данных (Big Data) и создавать индивидуальные образовательные «маршруты»;

– голосовые помощники («электронные ассистенты»), помогающие овладеть цифровыми технологиями в рамках игровых образовательных программ;

– VR&AR («виртуальная и дополненная реальность»), которая связывает дистанцированных субъектов образования и помогает им коммуницировать в увлекательной игровой форме в рамках виртуальных «интернет-аудиторий».

Однако несмотря на очевидные преимущества, цифровизация образования несет в себе определенные риски. К их числу специалисты относят: а) высокую цену виртуального оборудования при невысоком качестве учебного контента, который не всегда отвечает образовательным целям; б) захват образовательного пространства «информационными» игроками (информационными агрегаторами); в) вероятное сокращение рабочих мест; г) негативное влияние технологических новаций на ментальное пространство (см. выше) [Ломоносовские чтения, 2019, с. 585–586].

Формирование цифровой ментальности в значительной степени происходит в ходе «онлайн-образования». Результативность последнего во многом зависит от успешного развития корпоративного онлайн-обучения; обеспечения конкурентоспособности в области экспорта образовательных услуг; ориентации на стратегию развития человеческого капитала; применения иностранных языков в образовательных программах [Ломоносовские чтения, 2019, с. 488–489].

## Образовательные и ментальные аспекты национальной безопасности

Понятие «безопасность» можно трактовать как «положение, состояние и функционирование объекта, при котором наличие и действие деструктивных факторов не влечет его деформации… исключается или нейтрализуется возможность причинения… какого-либо ущерба, вреда либо придания его развитию нежелательных динамики или параметров» [Фельдман, 2011, с. 21]. Такая трактовка безопасности представляется особенно актуальной в условиях «общества риска», в ко-

тором разработка и применение все более совершенных технологий порождает угрозы его жизнедеятельности [Фельдман 2011, с. 34], поскольку предполагает способность и постоянную готовность социума к адекватному ответу на новые вызовы.

Особую роль в обеспечении безопасности играет сфера образования, в рамках которой создаются «глубинные механизмы самоопределения и информационно-культурного иммунитета», воспроизводится интеллектуальный потенциал общества [Фельдман, 2011, с. 24–25]. В свою очередь, необходимы гарантии безопасности и для самого образовательного пространства. Они обеспечиваются как непосредственно субъектами образования, так и представителями других отраслей, в первую очередь сферы культуры и систем жизнеобеспечения. Это предполагает проведение соответствующей политики и своевременную реализацию концепции или системы взглядов на защиту всех участников образовательного процесса от угроз для их жизни и здоровья [Золотухин, 2018, с. 117].

Очевидна связь безопасности образовательного пространства с национальной безопасностью. Национальная безопасность является необходимым условием формирования, развития и функционирования образования, в то время как образовательный потенциал представляет собой важнейший ресурс и инструмент национальной безопасности. Стратегическая значимость образования для обеспечения национальной безопасности объясняется, в первую очередь, тем, что оно формирует культуру безопасности на личном, групповом и государственном уровне.

На современном этапе цифровизации цель государственной политики в области безопасности образовательного пространства заключается в обеспечении безопасного доступа к качественным образовательным ресурсам. Ее достижение предполагает за счет комплексного применения различных инструментов правового, экономического и организационного характера [Фельдман, 2011, с. 17–18]. Основными задачами являются [Золотухин, 2018, с. 119–120]:

– разработка и внедрение нормативно-правовых, научно-методических и организационных основ формирования безопасного образовательного пространства;

– межведомственный, комплексный и многоуровневый подход к формированию безопасной учебной среды;

– совершенствование профессиональной компетентности и механизмов аттестации субъектов обеспечения безопасности;

– создание соответствующих социальных условий, поддерживающих комплексную безопасность всех участников образовательного процесса;

– выработка критериев эффективности функционирования отрасли образования в системе национальной безопасности.

Системный подход к проблеме безопасности предполагает введение понятия о ментальном иммунитете [Сидоров, 2015, с. 82], а также учет аксиологических целей и нравственных ориенти-

ров развития общества и государства. Для обеспечения ментальной безопасности, которую можно определить как «безопасный инжиниринг и менеджмент индивидуального и общественного сознания» [Сидоров, 2015, с. 87] и / или «нравственную устойчивость личности и общества к деструктивному воздействию…» [Миронов, Никитина, 2017, с. 183], разработаны и применятся различные инструменты. Например, на предотвращение угроз цифровизации направлены следующие когнитивные модели: «глубокая защита» (Defense in Depth), «цепочка киберубийства» (Cyber Kill Chain), «намерение доказательства» (Evidence Intention) и т.д. [Сандерс, 2019].

К основным показателям ментальной безопасности отечественные специалисты относят: уровень преступности и насилия, а также бедности, безработицы и социального расслоения в обществе. Кроме того, анализируется количество ментальных и социальных эпидемий; сочетание здорового образа и нравственного смысла жизни; баланс общечеловеческих и национальных ценностей и целей; адаптивность «профессиогенеза» и непрерывность образования; эффективность «самоменеджмента»; сформированность, стабильность и реализованность нравственных чувств, позиции и поведения; степень патриотизации и т.п. [Сидоров, 2015, с. 87–88].

Ментальная безопасность, которую можно рассматривать как ментальное измерение национальной безопасности, выполняет следующие функции: 1) регулятивную (обеспечивает управление различными ресурсами безопасности); 2) интегративную (аккумулирует разные уровни ментального иммунитета – от личности до социума); 3) адаптивную (обеспечивает приспособление к постоянно изменяющимся внешним и внутренним условиям и ресурсам безопасности); 4) резонансную (подразумевает приспособление к вызовам цифровизации); 5) кумулятивную (состоит в постепенном накоплении и моментальной мобилизации защитных ресурсов в критические периоды); 6) прогностическую и 7) интериоризационную или формирующую «внутренние паттерны защиты через усвоение внешних алгоритмов» [Сидоров, 2015, с. 86].

Эксперты подчеркивают взаимосвязь между ментальной и экономической безопасностью. Этот механизм в общем виде можно представить следующим образом: экономический менталитет включает культурные навыки хозяйственной деятельности, которые, в свою очередь, влияют на экономическую безопасность. В контексте цифровизации выделяют индивидуальные и общекультурные (ментальные) угрозы экономической безопасности. Первые состоят из деформаций в сознании индивидуума, вызванных оторванностью финансовой сферы от производства, недостаточно развитой мотивацией к эффективному экономическому поведению (способам сбережения и накопления) и т.п. Вторые предполагают искажения в общественном сознании, которые могут приносить ущерб национальной экономике, например в результате «утечки капитала» и т.п. [Прудникова, 2015].

Обеспечение ментального аспекта национальной безопасности в условиях цифровизации должно предусматривать реализацию соответствующей стратегии, которая включает следующие элементы [Сидоров, 2015, с. 91–93]:

– саморазвитие (личности, общества и т.д.);

– «адаптивное расширение сознания» по отношению к актуальным событиям;

– перманентная самоидентификация или сохранение восприятия своей личности при изменении социальных условий;

– асимметричная когерентность, заключающаяся в системности и целостности восприятия реального и виртуального мира при безусловном приоритете первого.

Обеспечение ментальной безопасности общества является не только информационно-технологической и правовой, но и педагогической задачей, поскольку деструктивное воздействие (в том числе экстремистских и криминальных групп) направляется, в первую очередь, на молодежь [Миронов, Никитина, 2017, с. 183]. В связи с этим необходима образовательная профилактика деструктивных воздействий на ментальное пространство, включающая превентивные меры духовно-нравственного, патриотического воспитания и образования. Именно такие образовательные (педагогические) практики могут стать базой для эффективного противодействия негативным цифровым эффектам (например, информационному экстремизму), а также инструментом комплексного обеспечения национальной безопасности в условиях цифровизации.

## Заключение

Процессы цифровизации затрагивают не только материально-техническую сферу, но и ментальное пространство современного социума, аккумулирующее аксиологические и когнитивные составляющие индивидуального и общественного сознания. Позитивное влияние цифровизации проявляется в совершенствовании кадрового потенциала, преумножении интеллектуального капитала, личностном и социальном прогрессе. Одновременно распространение цифровых технологий продуцирует и целый ряд негативных феноменов ментального пространства (ментальные вирусы и эпидемии, ментальные расстройства, культурную гипертекстуальность, деструктивные социальные группы, «клиповое мышление», фрагментацию социума и т.д.).

Образование является важнейшим фактором формирования цифровой ментальности (современного ментального пространства), при условии сохранения и адаптации фундаментальных традиционных образовательных форм и внедрения новейших образовательных методов и инструментов.

На современном этапе развития обеспечение безопасности государства зависит от потенциала образовательного пространства, которое включает знания, умения и навыки, накопленные социумом; образовательную систему и инфраструктуру; политико-административные нормы образовательной деятельности. Безопасность ментального пространства является ментальным (когни-

тивно-аксиологическим, духовным) измерением национальной безопасности, обеспечение которого зависит от эффективной реализации всех элементов соответствующей стратегии – самоактуализации, «адаптивного расширения сознания», самоидентификации, системности и целостности восприятия мира.

Комплексный подход к национальной безопасности предполагает гарантию ее ментальных и образовательных аспектов путем своевременного применение всей совокупности средств и ресурсов социума в соответствии с условиями повсеместной цифровизации общества в XXI в.

## Список литературы

Актуальные проблемы менеджмента: производительность, эффективность, качество // Материалы международной научно-практической конференции. – Санкт-Петербург, 2017. – 10.11. – URL: https://dspace.spbu.ru/bitstream/11701/9155/1/сб-Актуальные%20 проблемы%20 менеджмента-2017. pdf (Дата обращения: 11.03.2020.)

*Богданова А.А.* Формирование менталитета личности: учет универсального и специфического // Современные проблемы науки и образования. – 2015. – № 4, 10.07. – URL: https://www.science-education.ru/ru/article/view?id=20459 (Дата обращения: 11.03.2020.)

Вызовы цифровой экономики: итоги и новые тренды: сборник статей II Всероссийской научно-практической конференции. – Брянск: Брян. гос. инженерно-технол. ун-т, 2019. – 696 с.

*Дзялошинский И.М.* Российский журналист в посттоталитарную эпоху. Некоторые особенности личности и профессиональной деятельности. – М.: Восток, 1996. – URL: http://www.dzyalosh.ru/01-comm/books/russ-jornal/4-1.html (Дата обращения: 10.03.2020.)

*Золотухин М.А.* Концепция безопасности образовательного пространства // Технико-технологические проблемы сервиса. – 2018. – № 1(43). – С. 117–120.

*Ирисханова О.* Ментальное пространство // СКОДИС Центр социокогнитивных исследований дискурса при МГЛУ. – URL: http://scodis.ru/студентам/глоссарий/ментальное-пространство/ (Дата обращения: 10.03.2020.)

Ломоносовские чтения-2019. Секция экономических наук. Экономические отношения в условиях цифровой трансформации: сборник тезисов выступлений. – М.: Экономический факультет МГУ имени М.В. Ломоносова, 2019. – 1046 с. – URL: https://www.econ.msu.ru/sys/raw.php?o=56275&p=attachment (Дата обращения: 10.03.2020.)

*Миронов И.Л., Никитина С.С.* Ментальная безопасность России: педагогические аспекты // Вестник Санкт-Петербургского Университета МВД России. – 2017. – № 3 (75). – С. 182–184.

*Осорина М.В.* Ментальные пространства как психическая реальность // Вестник СПбГУ. Психология и педагогика. – 2017. – Т. 7, вып. 1. – С. 6–24.

*Почепцов Г.* Как информационные технологии атакуют ментальное пространство человечества // ResearchGate GmbH. – 2018. – 05.11. – URL: https://www.researchgate.net/publication/328738753_Kak_informacionnye_tehnologii_atakuut_mentalnoe_prostranstvo_celovecestva (Дата обращения: 11.03.2020.)

*Прудникова А.С.* Экономический менталитет как основной фактор личной экономической безопасности // Электронный научно-практический журнал «Психология, социология и педагогика». – 2015. – 06. – URL: http://psychology. snauka.ru/2015/06/5352 (Дата обращения: 12.03.2020.)

*Сандерс К.* Ментальные модели в информационной безопасности // Хабр. Сообщество IT-специалистов. – 2019. – 03.06 – URL: https://habr.com/ru/post/454596/ (Дата обращения: 12.03.2020.)

*Сидоров П.И.* Синдром приобретенного ментального иммунодефицита // Медицинский академический журнал. – 2015. – Т. 15, № 4. – С. 82–95.

Современная когнитология и когнитивная аналитика в контексте философской инноватики / научн. ред. проф. А.М. Старостин. – Ростов н/Д.: Изд-во ЮРИУ РАНХиГС, 2014. – 228 с.

*Фельдман О.А.* Образовательный потенциал системы национальной безопасности России: автореф. дис. … д-ра полит. наук. – 2011. – URL: http://cheloveknauka.com/obrazovatelnyy-potentsial-sistemy-natsionalnoy-bezopasnosti-rossii (Дата обращения: 10.03.2020.)

Что такое ментальность: здоровье и болезнь на ментальном уровне // KtoNaNovenkogo.ru. – 2019. – 04.10. – URL: https://ktonanovenkogo.ru/voprosy-i-otvety/mentalnost-chto-ehto-takoe-entalnogo-rasstrojstva-zdorovya.html (Дата обращения: 11.03.2020.)

*Шамаев А.Э.* Концепция ментальных пространств как способа организации прагматических значений в интеллектуальных системах, использующих ее // Компьютерная лингвистика и интеллектуальные технологии. – 2002. – URL: http://www.dialog-21.ru/digest/2002/articles/shamaev/ (Дата обращения: 12.03.2020.)

# ПРАВОВЫЕ МЕХАНИЗМЫ БИОБЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

**Карцхия Александр Амиранович**

Доктор юридических наук, профессор кафедры гражданского права РГУ нефти и газа (НИУ) им. И.М. Губкина (Москва, Россия)

***Аннотация***. *Новая технологическая среда, создаваемая цифровыми технологиями, позволяет совершать прорывные открытия во всех научных направлениях, но особенно – в биологических дисциплинах. С одной стороны, это дает надежду на решение множества проблем, начиная от лечения сложных заболеваний и заканчивая сферами энергетики и утилизации отходов. С другой стороны, биоинженерные технологии несут в себе серьезные угрозы и риски. В статье рассматриваются формирующиеся правовые механизмы в сфере биологической безопасности и правовые аспекты предотвращения биологических угроз в современном мире на национальном и международном уровне. Автор приходит к выводу о необходимости совершенствования национального законодательства и важности международного сотрудничества в этой области.*

***Ключевые слова:*** *цифровизация; биотехнологии; биологическая безопасность; биологическая защита; международное сотрудничество; коронавирус.*

**Для цитирования:** Карцхия А.А. Правовые механизмы биобезопасности // Социальные новации и социальные науки. – Москва: ИНИОН РАН, 2020. – № 1. – С. 119–127.

URL: https://sns-journal.ru/ DOI: 10.31249/snsn/2020.01.09

## Введение

Создание и широкое использование современных цифровых и иных «прорывных» технологий породило так называемую четвертую промышленную революцию, или «цифровую революцию», которая последовательно формирует новую социальную, экономическую, политическую и правовую реальность. Использование обширных возможностей в сфере IT-технологий и Интернета вещей создает особую технологическую и социально-экономическую среду [The Internet of Things, 2015]. Одновременно возникает множество вопросов в области правового регулирования применения цифровых технологий, охраны интеллектуальной собственности и защиты интеллектуальных прав [Цифровая экономика, 2019; Цифровые права, 2019].

Цифровизация разнообразных областей человеческой деятельности и применение связанных с ней передовых технологий определили возникновение принципиально нового поля гражданско-правового регулирования [Карцхия, 2019], а также потребность в адаптации существующей нормативной правовой базы. Это обусловило возрастающий научный интерес к общетеоретическим и научно-практическим исследованиям в области правового регулирования новых технологий в целях предотвращения вызванных их использованием рисков и угроз.

### Биотехнологии и вопросы обеспечения безопасности

Одной из наиболее быстро развивающихся высокотехнологических областей, обладающей огромным экономическим и военным потенциалом, в настоящее время считается сфера биотехнологий (Biotech). Не случайно XXI в. называют веком биомедицины. Бурное развитие получили созданные при помощи цифровых технологий генетические, тканевые и иные технологии, способные изменить парадигму лечебно-диагностического процесса, подходы к профилактике и реабилитации целого ряда заболеваний человека [Сергеев, Мохов, Яворский, 2019].

Однако эти же технологии способны нанести колоссальный вред и несут в себе огромную угрозу безопасности общества и государства. В связи с этим, например, Разведывательное сообщество США включило технологию редактирования генома в список «оружия массового уничтожения» («weapons of mass destruction»). В Программе развития цифровой экономики в РФ до 2035 г., разработанной Аналитическим центром при Правительстве РФ, отмечается, что мы находимся на пороге революции, превращающей жизнь в информацию, которая может быть написана и переписана так же, как компьютерный код. В течение следующих 30 лет синтетическая биология представит инженерные организмы, которые смогут обнаруживать токсины, выделять биотопливо из промышленных отходов, а также создавать лекарства, образующие симбиоз с людьми. В то же

время синтетическая биология представляет собой серьезные риски, включая искусственное биологическое оружие и инвазивные синтетические организмы, которые могут разрушать природные экосистемы [Программа …, 2017].

Готова ли Россия и мировое сообщество в целом обеспечить биозащищенность граждан? Обеспечивает ли существующее правовое регулирование достаточные гарантии для противодействия биологическим угрозам, возникающим в новой цифровой реальности? Пандемия коронавируса COVID-19, который появился в конце 2019 г. в Китае, стала настоящим испытанием готовности человечества противостоять биологическим угрозам.

Характерно, что Всемирная организация здравоохранения (ВОЗ) разделяет биозащищенность (Biosafety) и биобезопасность (Biosecurity) [Fact Sheet …, 2018]. Биозащищенность (Biosafety) означает принципы, технологии и методы сдерживания, которые применяются для предотвращения непреднамеренного воздействия патогенов и токсинов или их случайного высвобождения, что связано с рисками инфицирования работников медико-биологических лабораторий и третьих лиц по причине неисправного оборудования, ненадлежащих способов проведения работ или экспериментов (ненадлежащей обработки воздуха или систем обеззараживания отходов). Биобезопасность (Biosecurity) понимается как институциональные и личные меры безопасности, направленные на предотвращение потери, кражи, неправильного использования, утечки или преднамеренного высвобождения патогенов и токсинов при нарушении мер доступа к объектам, хранения материалов и данных, а также на обнародование информации о способах их создания. Основные риски в этом случае связанны с утратой или путаницей образцов, «воскрешением» уже вымерших вирусов и созданием вирусов, от которых нет вакцин или которые являются устойчивыми к лекарственным препаратам.

Наиболее серьезные угрозы связывают с биологическим оружием и биотерроризмом, который выражается в использовании высокопатогенных и инфекционных бактерий, вирусов и токсинов в военных и иных террористических операциях с целью вызвать инфекцию, болезни и смертность среди людей, животных или растений, поставить под угрозу социальную стабильность и национальную безопасность государства. Незаметность, разнообразие и скорость воздействия биологического оружия затрудняют его раннюю диагностику и медицинскую идентификацию. Кроме того, вредные эффекты биологического оружия имеют сильные ситуативные особенности применения в зависимости от видов патогенных микроорганизмов, способов биоатаки, социальных, природных и других условий, которые приводят к различным путям эволюции и уровня риска, усложняющим биологическую защиту.

Следует отметить, что международная Конвенция о запрещении разработки, производства и накопления запасов бактериологического (биологического) и токсинного оружия и об их уничто-

жении 1975 г. (Biological Weapons Convention) (далее – Конвенция) не содержит положений об эффективных средствах проверки и не запрещает разработку биологического оружия в оборонительных целях. Тем не менее Конвенция возлагает на государства-участники обязанности никогда, ни при каких обстоятельствах не разрабатывать, не производить, не накапливать, не приобретать каким-либо иным образом и не сохранять: 1) микробиологические или другие биологические агенты или токсины, которые не предназначены для профилактических, защитных или других мирных целей; 2) оружие, оборудование или средства доставки, предназначенные для использования таких агентов или токсинов во враждебных целях или в вооруженных конфликтах [Резолюция …, 1971]. При этом в дополнительных протоколах к Конвенции содержатся требования о даче разрешений на проведение медико-биологических исследований и получение на них информированного согласия пациента.

Определенным средством противодействия биотерроризму служит Всеобщая декларация о биоэтике и правах человека (ЮНЕСКО, 2005), которая не только декларирует обязанности сохранять биоразнообразие в качестве общей задачи человечества, но и требует от государств-участников принятия надлежащих мер для борьбы с биотерроризмом и незаконным оборотом органов, тканей, образцов, генетических ресурсов и генетических материалов.

## Опыт стран мира по обеспечению биологической безопасности

В последние годы в ряде стран мира приняты или модифицированы специальные законы о биологической защите. В частности, в *Новой Зеландии* в новой редакции принят Закон о биологической безопасности (Biosecurity Law Reform Act 2012), а также Закон об исключительной экономической зоне, применяемый в целях предотвращения проникновения вредителей и нежелательных микроорганизмов в страну [Biosecurity Law Reform Act, 2012].

В 2019 г. в *Австралии* принята новая редакция Закона о биобезопасности 2015 (Biosecurity Act 2015), заменяющая Закон «О карантине» (Quarantine Act 1908). Она регламентирует управление широким спектром рисков биозащиты человека, включая заражения опасными болезнями и проникновение определенных болезней на территорию страны, а также рисков, связанных с загрязнением подземных вод и чрезвычайными ситуациями в биосфере. Кроме того, определяет порядок реализации международных прав и обязательств Австралии, в том числе международных медико-санитарных правил (International Health Regulations 2005), соглашения ВТО о применении санитарных и фитосанитарных мер (Agreement on the Application of Sanitary and Phytosanitary Measures) и Конвенции о биологическом разнообразии (Convention on Biological Diversity 1992) [Glowka, 1994].

В *Китае* рассматривается проект закона о биологической безопасности, который направлен на обеспечение безопасности национальных биоресурсов, стимулирование и защиту развития био-

технологий, а также предотвращение и запрет применения биологических агентов или биотехнологий, которые могут нанести ущерб национальной безопасности КНР [Проект закона КНР ..., 2020].

Стратегические документы *ЕС* по биоэкономике [Bioeconomy Strategy, 2018; Innovating for …, 2012] отмечают необходимость искать новые способы производства и потребления, которые наиболее полно учитывают экологическую безопасность в условиях ограниченных ресурсов и глобальных вызовов, таких как изменение климата, деградация земель и экосистем в сочетании с растущей численностью населения планеты.

Кроме того, в последние годы были обнародованы официальные национальные стратегии биологической безопасности ведущих стран в сфере биотехнологий и биомедицины – Великобритании и США, – в которых выражается озабоченность по поводу биозащиты.

В сентябре 2018 г. в *США* утверждена Национальная стратегия биологической защиты (National Biodefense Strategy) (далее – Стратегия) для защиты США от биологических угроз, предотвращения биоинцидентов (bioincidents) и борьбы с их последствиями, а также многоуровнего управления рисками, связанными с естественными, случайными или преднамеренными биологическими угрозами для общества, экономики и окружающей среды. Как отмечено в меморандуме Белого дома, Стратегия неразрывно связана с Национальной стратегий безопасности США (National Security Strategy, 2018) и основывается на уроках, извлеченных из прошлых биологических инцидентов. Стратегия направлена на создание более жизнеспособного и эффективного механизма биологической защиты нации от биологических угроз, которые исходят из многих источников, не знают границ и обладают огромным потенциалом для разрушения экономики, нанесения ущерба человеческой жизни и разрушения самой структуры общества [National biodefense strategy, 2018].

В Стратегии выделены два типа биологических угроз. Во-первых, естественные биологические угрозы, т.е. угрозы инфекционных заболеваний, которые носят трансграничный характер. Во-вторых, преднамеренные и случайные биологические угрозы, которые выражаются в применении биологического оружия или его распространении государственными или негосударственными субъектами, представляющие серьезную угрозу национальной безопасности, населению, сельскому хозяйству и окружающей среде. В Стратегии указывается, что многие страны осуществляли тайные программы по созданию биологического оружия, а ряд террористических групп стремился приобрести биологическое оружие. Во многих странах мира патогенные микроорганизмы хранятся в лабораториях, где отсутствуют надлежащие меры биозащиты, что может привести к нанесению вреда.

Управление биологическими рисками является важным элементом Стратегии. Отмечается, что требуется понимание и оценка биологических рисков, а также реагирование на них и принятие мер по предотвращению, независимо от того, имеют место они в США или за рубежом. Стратегия основывается на том, что биологические угрозы нельзя свести к нулю, но этими рисками можно и нужно управлять. С помощью Стратегии правительство США оптимизирует свои собственные усилия и организует работу партнеров внутри страны и за ее пределами для противодействия всему спектру биологических угроз.

Аналогичный межведомственный подход к биологической безопасности принят в Стратегии биологической безопасности *Великобритании* (UK Biological Security Strategy), опубликованной в августе 2018 г. Цель данной Стратегии состоит в защите страны и ее интересов от существующих основных биологических угроз, независимо от их источников и объектов влияния. Подчеркивается, что межведомственный совет, подотчетный подкомитету Национального Совета безопасности, будет способствовать развитию существующих механизмов управления угрозами и противодействию им [UK Biological Security Strategy, 2018].

## Законодательство РФ в области обеспечения биологической безопасности

Выработке правовых основ национальной биологической безопасности в России придается большое значение. Активизация законотворческой деятельности в этой области связана, прежде всего, с тем, что в настоящее время отсутствует комплексное регулирование этих вопросов. Необходимо создание системы взаимоувязанных мер, функционирующей на основе взаимодействия заинтересованных органов государственной власти в целях противодействия возникновению биологических угроз, организации защиты населения и охраны окружающей среды, а также ликвидации последствий воздействия опасных биологических факторов. Нарастание в современном мире биологических угроз различного рода требует формирования единых межотраслевых подходов в сфере биологической защищенности и безопасности, а также их законодательного закрепления для эффективного функционирования системы обеспечения биологической безопасности в РФ.

В целях реализации «Основ государственной политики РФ в области обеспечения химической и биологической безопасности на период до 2025 года и дальнейшую перспективу» в 2019 г. в Государственную думу внесен на рассмотрение проект Федерального закона «О биологической безопасности Российской Федерации» [Проект федерального закона …, 2019] (далее – Законопроект). Он восполняет существующие пробелы для однозначного толкования и формирования единой правоприменительной практики, определяя содержание деятельности по обеспечению биологической безопасности, в том числе путем введения понятийного аппарата, в настоящее время отсутствующего в законодательстве [Пояснительная записка …, 2019]. Принципиальным моментом является межотраслевой, комплексный характер Законопроекта, который включает охрану здоро-

вья и санитарно-эпидемиологическое благополучие населения, защиту животных и растений, охрану окружающей среды.

Законопроект устанавливает понятие «биологическая безопасность» как состояние защищенности населения и окружающей среды от воздействия опасных биологических факторов, при котором обеспечивается допустимый уровень биологического риска. Формулируются также основные биологические угрозы (опасности), с которыми связаны биологические риски, представляющие собой вероятность причинения вреда (с учетом его тяжести) здоровью человека, животным, растениям и (или) окружающей среде в результате воздействия опасных биологических факторов [Проект федерального закона …, 2019].

В то же время, по мнению некоторых специалистов, «концепция экологической безопасности через «состояние защищенности» безнадежно устарела и не сопрягается (гармонизируется) ни с устойчивым развитием, ни с экономическим развитием, ни с ценностными установками, ни с концепцией глобализации» [Жаворонкова, Агафонов, 2019, с. 107]. Предлагаемое понимание термина «безопасность» применительно к экологическим проблемам через концепцию «устойчивого развития» в виде нового термина «безопасное устойчивое развитие» (которое может применяться и к генетической и биосферной безопасности) не раскрывает смысл биобезопасности. Вероятно, научную дискуссию по этому вопросу следует продолжить.

Эксперты отмечают, что в современных условиях международное сотрудничество и национальное правовое регулирование в сфере биологической безопасности не может ограничиваться только укреплением режима Конвенции или других международных договоров. Требуется установить правовые рамки для генетических исследований, диагностики и скрининга генома, а также трансплантации органов и тканей человеческого происхождения, исследований человеческих эмбрионов in vitro [Международно-правовое регулирование …, 2019; Романовский, 2016].

## Заключение

Как стало очевидным, в современном мире необходимость в биологической безопасности значительно выше, чем когда-либо в прошлом. На национальном и глобальном уровнях биобезопасность определяется способностью эффективно реагировать на биологические угрозы и связанные с ними факторы способностью поддерживать и защищать безопасность и интересы граждан. Этот механизм включает в себя меры предотвращения и борьбы с основными инфекционными заболеваниями, защитные меры против биологического оружия, систему предотвращения актов биологического терроризма и злоупотребления достижениями биотехнологий, защиту биологической безопасности лабораторий, специальных биологических ресурсов и предотвращение вторжения чужеродных опасных для человека и окружающего его мира организмов.

Сейчас выдвигаются новые требования к возможностям биологической защиты, таким как наличие аварийного персонала, средств защиты первой необходимости, специальных лекарственных препаратов и вакцины, оборудования для лечения, системы мониторинга и раннего оповещения, а также утилизация, восстановление и реконструкция места биологической атаки. Особую актуальность приобретают правовые аспекты технологий биобезопасности.

Глубокие изменениями в области международной безопасности, глобализация, цифровизация и развитие биотехнологий обусловили разработку в РФ проекта федерального закона о биологической безопасности. Данный законопроект является реакцией на возникновение новых рисков и проблем, связанных с инфекционными заболеваниями, биотерроризмом и другими современными угрозами биобезопасности и биозащищенности.

Обеспечение биологической безопасности требует системного подхода и организации, что предусматривает целый комплекс мер, закрепленный в специальных законодательных актах национального уровня. Они также должны быть скоординированы на уровне международных конвенций по вопросам биобезопасности.

## Список литературы

*Жаворонкова Н.Г., Агафонов В.Б.* Теоретико-методологические проблемы правового обеспечения экологической, биосферной и генетической безопасности в системе национальной безопасности Российской Федерации // Lex russica. – 2019. – № 9. – С. 96–108.

*Карцхия А.А.* Гражданско-правовая модель регулирования цифровых технологий: диссертация на соискание ученой степени доктора юридических наук. – М., 2019. – 394 с.

Международно-правовое регулирование предымплантационной генетической диагностики (ПГД) и тенденции развития российского законодательства в сфере вспомогательных репродуктивных технологий / Алтынник Н.А., Комарова В.В., Бородина М.А., Суворова Е.И., Зенин С.С., Суворов Г.Н. // Lex russica. – 2019. – № 6. – С. 9–17.

Пояснительная записка к Проекту федерального закона № 850485–7 «О биологической безопасности Российской Федерации» // Государственная Дума РФ. Официальный сайт. – 2019 – URL: https://sozd.duma.gov.ru/bill/850485-7 (дата обращения 25.02.2020).

Программа развития цифровой экономики в Российской Федерации до 2035 года // Аналитический центр при Правительстве РФ. – 2017 – URL: http://spkurdyumov.ru/uploads/2017/05/strategy.pdf (дата обращения 25.02.2020).

Проект закона КНР о биологической безопасности представлен на рассмотрение ПК ВСНП во втором чтении // russian.people.cn. – 2020. – 27.04. – URL: http://russian.people.com.cn/n3/2020/0427/c31521-9684284.html (дата обращения 25.02.2020).

Проект федерального закона № 850485–7 «О биологической безопасности Российской Федерации» // Государственная Дума РФ. Официальный сайт. – 2019 – URL: https://sozd.duma.gov.ru/bill/850485-7 (дата обращения 25.02.2020).

Резолюция Генеральной Ассамблеи ООН, принята на двадцать шестой сессии. 21 сентября – 22 декабря 1971 г. // Генеральная Ассамблея. Официальные отчеты. Двадцать шестая сессия. Дополнение N 29 (A/8429). – Нью-Йорк: Организация Объединенных Наций, 1973. – С. 34–36.

*Романовский Г.Б.* Правовое регулирование генетических исследований в России и за рубежом // Lex russica. – 2016. – № 7. – С. 93–102.

*Сергеев Ю.Д., Мохов А.А., Яворский А.Н.* Пилотный (экспериментальный) правовой режим для отечественной биомедицинской науки и практики // Медицинское право. – 2019. – № 4. – С. 3–13.

Цифровая экономика. Проблемы правового регулирования / отв. ред. В.В. Зайцев, О.А. Серова. – М.: Кнорус, 2019. – 200 с.

Цифровые права как новый объект гражданского права. Комментарии экспертов // Закон. – 2019. – № 5. – С. 31–55.

Bioeconomy Strategy. A sustainable bioeconomy for Europe: strengthening the connection between economy, society and the environment // European Commission. – 2018. – URL: https://ec.europa.eu/research/bioeconomy/pdf/ec_bioeconomy_strategy_2018.pdf (дата обращения 25.02.2020).

Biosecurity Law Reform Act 2012 // Parliamentary Counsel Office of the New Zealand. – 2012. – URL: http://www.legislation.govt.nz/act/public/2012/0073/latest/whole.html (дата обращения 25.02.2020).

Fact Sheet. Biosafety and Biosecurity // WHO. – 2018.–20.03. – URL: https://www.who.int/ (дата обращения 25.02.2020).
Global Innovation Index 2016: Winning with Global Innovation // Cornell University, INSEAD, The World Intellectual Property Organization (WIPO). – Geneva, 2016. – URL: http://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2016 (дата обращения 25.02.2020).
Global Innovation Index 2017: Innovation Feeding the World // Cornell University, INSEAD, The World Intellectual Property Organization (WIPO). – Geneva, 2017. – URL: http://www.wipo (дата обращения 25.02.2020).
*Glowka L., Burhenne-Guilmin F., Synge H.* A Guide to the Convention on Biological Diversity // International Union for Conservation of Nature and Natural Resources and Cambridge. – 1994. – URL: https://portals.iucn.org/library/efiles/documents/EPLP-no.030.pdf (дата обращения 25.02.2020).
Innovating for Sustainable Growth: A Bioeconomy for Europe // European Commission. – 2012. – URL: https://op.europa.eu/en/publication-detail/-/publication/1f0d8515-8dc0-4435-ba53-9570e47dbd51 (дата обращения 25.02.2020).
National biodefense strategy // White House of the USA. – 2018 – URL: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Biodefense-Strategy.pdf (дата обращения 25.02.2020).
The Internet of Things: Mapping the value beyond the hype // McKinsey Global Institute. – 2015. – URL: https://www.mckinsey.com (дата обращения 25.02.2020).
UK Biological Security Strategy // UK Government. – 2018. – URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/730213/2018_UK_Biological_Security_Strategy.pdf (дата обращения 25.02.2020).
WIPO Technology Trends 2019: Artificial Intelligence // The World Intellectual Property Organization (WIPO). – Geneva, 2019. – URL: http://www.wipo.int (дата обращения 25.02.2020).

# ЧЕЛОВЕК В ЦИФРОВОМ МИРЕ

## НОВЫЕ СИСТЕМЫ КОНТРОЛЯ И МОНИТОРИНГА

**Петров Александр Арсеньевич**

Доктор экономических наук, профессор, Московский государственный юридический университет имени О.Е. Кутафина (Москва, Россия)

***Аннотация***. *Развитие цифровых технологий ускорило разработку и применение новых систем наблюдения и контроля за населением. Уже действуют скоринговые системы в банковском секторе. Запускается система цифрового профиля физического и юридического лица в России. Как она будет использоваться, зависит от тех, кто принимает решение и кто эксплуатирует систему. Но главным носителем информации о себе остается сам человек.*

***Ключевые слова:*** *системы мониторинга; скоринг; цифровой профиль; безопасность цифровых технологий.*

**Для цитирования:** Петров А.А. Новые системы контроля и мониторинга // Социальные новации и социальные науки. – Москва: ИНИОН РАН, 2020. – № 1. – С. 128–142.

URL: https://sns-journal.ru/ DOI: 10.31249/snsn/2020.01.10

## Введение

Новые цифровые технологии позволяют объединять, обрабатывать и анализировать самую разнообразную и разностороннюю информацию, поступающую из множества источников. Благодаря этому в разных странах создаются современные системы контроля за гражданами и организациями, которые имеют типовой алгоритм и совершенствуются по мере развития цифровых систем. Степень контроля зависит от уровня демократизации общества и уровня защиты прав и свобод человека. Лидирующие позиции в организации тотального контроля (масштабного и всестороннего изучения и анализа настроения и поведения граждан со 100%-ным охватом) с использованием цифровых технологий, включая технологии искусственного интеллекта (ИИ-технологии), в настоящее время занимает Китай.

Стартовой площадкой для создания подобных контролирующих систем во всем мире является применяемая банками система «кредитная история», которая позволяет определять кредитоспособность заемщика и выяснять уровни риска, связанные с его кредитной активностью. Однако «кредитная история» охватывает только тех физических и юридических лиц, которые прибегают к банковским кредитам. Часть населения остается вне ее контроля. В семье с общим бюджетом кредит берет один член семьи, и остальные не попадают в поле зрения банков.

Следующим этапом является широкое распространение банковских карт, предоставляющих возможность проводить безналичные расчеты и отслеживать платежеспособность человека, что преодолевает ограниченность системы «кредитная история». Но и банковские карты не дают полной картины покупательской активности человека, поскольку ряд сделок-операций по тем или иным причинам оплачивается наличными средствами. Третьей составляющей стало совершенствование налоговой системы, следящей за уплатой налогов с официальных доходов. При этом в России пенсии государственного обеспечения, не подлежащие налогообложению (в соответствии с п. 2 ст. 217 НК РФ)[1], налоговой системой не учитываются. К тому же налоги уплачивают только лица, имеющие идентификационный номер налогоплательщика (ИНН). Хотя ИНН в России можно получить при рождении ребенка.

Дальнейшие шаги – перевод в цифровую форму уплаты штрафов и пеней за нарушение установленных норм и паспортизации населения. В Китае бумажные паспорта уже заменяются пожизненными электронными картами личности. В России с марта 2020 г. веден электронный паспорт.

[1] За исключением выплат из добровольного страхования накопительной части пенсии и пенсий негосударственного обеспечения (согласно нормам пп. 1 и 2 ст. 213.1 НК РФ).

Наконец, последовало внедрение цифровых технологий в процессы анализа разнообразной и разносторонней информации госорганов, торговых сетей, индустрии отдыха. Еще в начале XXI в. эти огромные массивы разрозненных данных на разнообразных носителях не поддавались интегрированному учету и обработке. С развитием науки о данных и совершенствованием цифровых технологий начались совмещение, обработка и анализ громадных непрерывно обновляемых потоков информации.

При этом не следует забывать: информация – это капитал, а ее использование – мощный инструмент в конкурентной борьбе и получении прибыли. Кроме того, информацию можно продавать и покупать.

## Скоринговая система

Банки всегда находились, находятся и будут находиться в поисках и совершенствовании технологий снижения риска кредитной активности. Одним из соответствующих этому направлению инструментов является кредитная история клиента, показывающая его обязательства, аккуратность или задержки погашения кредита, платежную дисциплину по бытовым платежам. В финансовом мире также давно применяется оценка кредитного рейтинга человека на основании его близкого окружения, или «риск связанности» – affinity risk. Сегодня эта система больше известна как программа «Приведи друга». Однако только кредитной истории в настоящее время уже недостаточно для принятия решения о выдаче кредита – требуются дополнительные данные о клиенте. Такие данные предоставляет скоринговая система.

Скоринговая модель или скоринговый портрет клиента (от англ. score – счет) – это система оценки потенциального клиента по параметрам, которые банк может отследить по банковской карте, в свободном интернет-доступе и в соцсетях, в том числе: 1) финансовое поведение клиента, его сбережения, накопления и траты, образ жизни; 2) платежи за границей, 3) портрет в социальных сетях, 4) информация от сотовых операторов, 5) информация от налоговых органов, 6) семейное положение, 7) образование и т.д.

Например, использование данных от сотовых операторов и систем платежей позволяет кредитным организациям уточнить данные о доходах клиента и узнавать, бывает ли он за границей. Широко применяется также психометрический скоринг, который с большой вероятностью позволяет выявить склонности, основные качества и паттерны (модель, стиль) поведения личности. С согласия клиента банки могут запрашивать юридически значимую информацию у государственных органов.

В США некоторые банки помимо стандартной информации о потенциальном заемщике включают в скоринг образование будущего клиента, сферу его деятельности и карьерный путь, стаж и опыт работы человека. В получении этой информации банкам помогает стартап UpStart

(Google). Кроме того, стартап Kabbage предоставляет выписку с PayPal-аккаунта и по покупкам на eBay и Amazon.

В России банки интересуются, зарегистрирован ли человек на сайте по поиску вакансий, ищет ли работу (значит, сидит «на мели»). Работающий клиент может вызвать подозрение, если заявленный доход не совпадает с вилкой зарплаты в его резюме [Леонидов, 2017].

В финансовой индустрии набирает популярность транзакционный скоринг, позволяющий банкам оценивать движение денежных средств на счетах клиента, категории его трат при оплате банковской картой и характер расчетов с компаниями и организациями.

Для определения кредитоспособности клиента банки работают с большими массивами данных. По результатам скоринговой оценки клиенту начисляются баллы, количество которых служит основанием для принятия банком решения о сотрудничестве с ним. Скоринг-балл – величина непостоянная, она может как снижаться, так и увеличиваться. Скоринговая система, во-первых, позволяет сразу отклонить заявку, по которой предоставление кредита невозможно – потеря работы, налоговая задолженность, небольшая заработная плата. Во-вторых, она может служить основой для предоставления индивидуальных льгот – устанавливать индивидуальную ссудную ставку, снижающуюся по мере роста скорингового балла.

Оперативное получение необходимой информации о клиентах в России стало возможным благодаря вступившей в силу 31 декабря 2019 г. поправке в Федеральный закон «О кредитных историях», согласно которой граждане могут получать персональный кредитный рейтинг и узнавать его вместе с отчетом бюро кредитных историй.

В России крупнейшая технологическая и поисковая IT-компания Яндекс совместно с бюро кредитных историй «Эквифакс» и Объединенным кредитным бюро» (ОКБ) запустили совместную программу «Интернет-скоринг бюро», позволяющую оценить кредитные риски, кредитоспособность и платежеспособность физических лиц. В данной программе Яндекс работает с большим объемом агрегированных и обезличенных статистических данных о своих пользователях, исключая предоставление конфиденциальной информации третьим лицам. По итогам анализа выдается только одно число – результат скоринговой оценки, имеющий рекомендательный характер и использующийся исключительно в маркетинговых целях.

В настоящее время скоринговая система может применяться для всестороннего сбора и анализа данных о любом гражданине, предпринимателе или компании. Опираясь на значение скорингового балла (суммы баллов, полученных в результате скоринговой оценки), организации могут выдавать или отказывать в кредите, принимать на данную должность или предлогать иную работу.

Основанные на математических и статистических алгоритмах технологии скоринговой обработки данных беспристрастны и исключают человеческий фактор. Плохое настроение работника,

невнимательность и предвзятость менеджера не влияют на рассмотрение заявки. Однако огромные массивы информации не всегда востребованы для принятия решения. Согласно закону Парето, достаточно 20% информации для принятия нужного решения. По мнению банковских работников, для этого иногда достаточно и 5% доступной информации. В то же время максимально большие объемы информации позволяют выявить закономерности поведения клиента.

Особую ценность для организаций и госструктур при анализе человека, отдельных групп людей и населения в целом представляют пять кластеров информации: 1) поведение клиента на сайте при заполнении анкеты / заявки – заполняет быстро или думает над каждым пунктом; 2) IP-адрес клиента, его браузеры и соцсети; 3) история поиска в сети Интернет; 4) черные списки открытых источников информации; 5) страницы и активность (продолжительность и регулярность входа) в социальных сетях.

В России, как и в других странах мира, скоринговые системы применяются для выявления неблагонадежных пассажиров и граждан других государств, находящихся в стране без регистрации. Скоринговые методы применяются также государствами и частными компаниями в социально-экономических целях.

В настоящее время модели кредитных скорингов широко применяются в здравоохранении, службах знакомств, при оценке клиента в системе автострахования, аренды жилья, найме на работу и предоставлении услуг сотовой связи. Агрегированная информация также полезна торговым платформам, которые создают собственные информационные системы оценки потенциальных клиентов.

Одним из скоринговых методов является репутационный скоринг. По мнению ряда специалистов, он позволяет более эффективно и адресно распределять социальные льготы физическим лицам, а также может применяться для оценки деятельности юридических лиц с целью повышения эффективности и стимулирования роста национальной экономики. В одних странах репутационный скоринг используются как источник информации о клиентах. В других он является составной частью системы государственного управления. Результаты скорингового оценивания применяются для выделения социальных льгот некоторым группам населения за счет средств муниципалитетов и городов. В качестве примера можно привести использование репутационного скоринга в Китае в рамках системы социального кредитования.

Востребованность скоринговых технологий балльно-рейтинговой оценки личности растет. Однако введение подобной системы репутационной оценки в России требует серьезного изменения национального законодательства.

Вместе с тем в России уже действует система «оператора фискальных данных» (ОФД), которая позволяет налоговому ведомству контролировать операции купли-продажи в режиме реально-

го времени (онлайн). В настоящее время она охватывает оптовую и розничную торговлю, но ее эффективность зависит от возможности маркировки продукции.

Использование цифровых технологий резко ограничило возможности ухода от налогообложения прибыли как юридических, так и физических лиц. В то же время система ОФД ставит под государственный контроль бюджеты домашних хозяйств. Одновременно она стимулирует развитие онлайн-сервисов и мобильных приложений в области контроля расходов, а также управление семейным бюджетом в целом.

### *Риски использования скоринговой системы*

С совершенствованием ИИ-технологий и нейросетей возможности систем мониторинга многократно возрастают. Собранная разнообразная и разносторонняя информация из многочисленных источников позволяет составить полный портрет человека с его предпочтениями, наклонностями и морально-психологическими качествами, детально определить потенциальные возможности, прогнозировать и управлять его будущим, в том числе финансовым поведением.

Главными «информаторами» для скоринга выступает сам человек, а также гаджеты, которыми он пользуется, и различные девайсы, его окружающие, проявления жизненной активности в виртуальном и реальном мирах. Важным источником информации является «добровольное» согласие человека на обработку персональных данных при обращении в интернет-магазин, организации здравоохранения и образовательные учреждения, визовые центры. По мнению экспертов, Google и Apple знают о своих пользователях больше государства, а по некоторым направлениям – больше самого человека [Может ли …, 2019].

Следует иметь в виду, что современные цифровые устройства – это не просто «железо», а, прежде всего, операционная система, которая следит за интернет-активностью пользователя и передает всю собираемую информацию на главный сервер. Деятельность подобного шпиона можно проиллюстрировать на примере операционной системы Windows 10, которая через учетную запись Microsoft: 1) отслеживает поведение пользователя в Интернете, включая местоположение и круг интересов; 2) анализирует посещаемые веб-сайты и сканирует загруженные файлы; 3) просматривает веб-контент, получает доступ к приложениям; 4) идентифицирует приложения с помощью рекламного идентификатора и отправляет информацию в компанию Microsoft; 5) отслеживает недавно используемые файлы и папки; 6) запоминает открываемые файлы и часто используемые папки.

Постоянно пополняющимся и бездонным источником информации являются социальные сети. Каждая из таких социальных сетей, как Facebook, Google+, Tumblr, Twitter, LinkedIn, Tencent Qzone, Sina Weibo, ВКонтакте, Одноклассники, Renren, имеет более 100 млн пользователей [Самые большие …, 2019]. Соцсети, открытые для всех и всегда, фактически охватывают все населе-

ние многих стран мира. Информация из соцсетей попадает в силовые структуры, налоговые органы, банковскую систему, коммерческие организации. Собранная информация также используется рекламодателями для разработки эффективной целевой рекламы, позволяя адресовать пользователю только те рекламные объявления, которые могут его заинтересовать. Соцсети сотрудничают со спецслужбами, передавая им досье о своих пользователях (о чем сообщил бывший сотрудник Агентства национальной безопасности США Э. Сноуден). Особую роль для отслеживания поведения пользователей играют cookie-файлы[1] и социальные плагины, как, например, кнопка «Нравится», «Подписаться» и другие, имеющиеся практически на каждом сайте. Такое аккумулирование информации является потенциальной угрозой конфиденциальности. Поэтому следует очень серьезно подумать, прежде чем размещать в соцсетях личную информацию.

Наглядно эту скрытую сторону соцсетей можно увидеть в отчете основателя Facebook М. Цукерберга: применяемые методы позволяют собирать информацию о владельце аккаунтов и о пользователе, у которого нет аккаунта; отслеживать движение мыши, уровень заряда батареи и мониторить устройства вблизи пользователя; анализировать контактную информацию, включая телефонную книгу, журнал звонков, SMS-переписку; отслеживать и архивировать информацию о локации GPS; собирать информацию об интернет-активности людей вне соцсети; иметь данные о провайдере интернет-услуг и мобильном операторе пользователя. По данным британской аналитической компании Cambridge Analytica, Facebook собрала личные данные более чем о 50 млн своих пользователей, и досье на пользователей на определенных условиях передаются некоторым организациям [Литвиненко, 2020].

С 2012 г. Facebook внедряет собственную систему авторизации и идентификации клиентов, учитывая их поведение в соцсетях с целью оценить надежность каждого по отношению к другим пользователям Сети и блокировать распространение нежелательной для клиента информации. Эту систему Facebook намерен трансформировать в кредитный скоринг и вывести ее на уровень кредитования членов соцсети с использованием рейтинговой информации о друзьях заявителя. Такое преобразование деятельности компании по законодательству США меняет ее статус и обязывает регулярно отчитываться в качестве финансовой организации перед надзорными органами.

Facebook также запустил программу предоставления банкам информации о профиле (портрете) пользователей Сети, которые могут стать их клиентами. Причем количество положительных контактов переходит в качество: чем больше контактов с надежной кредитной историей, тем выше шансы получить кредит по льготной ставке. Данная программа представляет внутренний скоринг социальной сети компании – Facebook-скоринг.

[1] Cookie-файлы – (англ. cookie, буквально – печенье) – небольшой фрагмент данных, отправленный вебсервером, хранимый на компьютере пользователя и собирающий данные о настройках, предпочтениях, данных авторизации и другую статистическую информацию [по материалам Википедии].

Уход из соцсетей и оплата покупок наличными не является гарантией защиты от проникновения в личную / частную жизнь. Люди все активнее пользуются мобильными телефонами, интернет-информацией, интернет-магазинами, проявляя нарастающую онлайн-активность. Все это становится базой данных для скоринга.

Скоринговая модель, как любое явление, имеет положительную и отрицательную стороны. Вторжение в личную жизнь и передача собранной информации коммерческим компаниям – это очевидные ее негативные аспекты, а передача данных о пользователях спецслужбам – тем более. Но последнее имеет и положительный эффект – борьба с терроризмом и экстремизмом, предотвращение терактов. Применение скоринг-технологий также существенно снижает масштабы мошенничества в банковском и страховом секторах, выступает основой совершенствования финансовой системы.

Одновременно возникает необходимость унификации информации, получаемой из различных систем, а также обеспечения ее достоверности и объективности. В распоряжении скоринговой системы находятся только те данные, которые сообщают о себе пользователи. Для проверки их достоверности программы анализируют частоту, качество, активность и постоянство связей клиентов.

### *Совершенствование технологий скоринга*

Биометрические технологии позволяют измерять уникальные характеристики отдельно взятого человека. Интеграция скоринга и биометрических технологий создает наиболее эффективную (непробиваемую или сверхнадежную) защиту во всех сферах деятельности человека и бизнеса.

В банковско-кредитной индустрии применяют такие биометрические технологии, как: 1) аутентификация по отпечаткам пальцев, 2) геометрия руки, 3) сопоставление речи клиента с его «голосовыми слепками», 4) сканирование сетчатки глаза, 5) динамика воспроизведения подписи или рукописного ключевого слова, 6) распознавание лица по фото, 7) ДНК, 8) рисунок вен. Биометрические технологии гарантируют более совершенную систему защиты финансов по сравнению с ПИН-кодом и СМС от банка.

Во многих странах мира предоставление биометрических данных служит основой безвизового режима. Например, США имеют соглашения с 27 странами о безвизовом режиме при обязательном наличии биометрических данных.

В России в рамках программы «Цифровая экономика» с 2018 г. действует Единая биометрическая система, распознающая личность человека по изображению и голосу. Кроме того, технология нейронной сети или уникальной системы нейронных связей в мозгу отдельного индивида может уже в 2030–2040 гг. использоваться наряду, а возможно, и вместо отпечатков пальцев для идентификации личности.

Вместе с тем сбор биометрических данных – это очень деликатный вопрос, – и данная процедура может осуществляться только при согласии человека (или на основании специального законодательного акта).

Новые технологии скоринга получили дополнительный импульс с развитием Data Science или науки о данных.

Data Science (нередко datalogy – даталогия) – междисциплинарная наука о данных, – является разделом информатики, изучающим широкий круг проблем, связанных с анализом, обработкой и представлением больших объемов разнообразных данных. Фактически наука о данных интегрирует различные методы статистики, обработки и интеллектуального анализа, проектирования и разработки баз данных, машинного обучения и оптимизации всего процесса принятия решения. Практическая цель науки о данных – выявить закономерности в данных и извлечь знания в обобщенной форме.

Алгоритмы машинного обучения позволяют выявить закономерности в данных, которые остаются вне поля зрения человека, а затем на этой основе строить прогнозы, разрабатывать проекты, планировать их реализацию и оценивать результативность решения конкретных задач. Система эффективно действует при непрерывном поступлении больших объемов информации. При небольших объемах поступающей периодически информации система дает сбой и допускает ошибки.

Например, 85% компаний списка Fortune 500[1] используют большие данные как основу для формирования конкурентных преимуществ. В свою очередь, профессия специалиста по Data Science с 2010 г. стала одной из самых высокооплачиваемых и перспективных в мире.

### *Цифровой профиль физического и юридического лица в России*

В инфраструктуру электронного правительства России входит Единая система идентификации и аутентификации (ЕСИА), частью которой является цифровой профиль физического и юридического лица или совокупность цифровых записей о гражданах и организациях, содержащихся в государственных информационных системах. Инфраструктура цифрового профиля обеспечивает возможность доступа к информационным системам в режиме «одного окна». При этом сам цифровой профиль постоянно пополняется и обновляется в режиме нон-стоп (каждые 15 секунд), сохраняя актуальность и достоверность данных. Систему цифрового профиля планируется запустить в конце 2020 г., а к 2023 г. его будут иметь все граждане России.

Цифровой профиль создается для повышения качества электронного взаимообмена между финансовыми институтами, бизнесом, государственными структурами и населением, упрощения и ускорения получения государственных и коммерческих услуг в режиме онлайн. Данные, собирае-

[1] Список 500 крупнейших компаний, базирующихся в США, который ежегодно составляется журналом Fortune. – *Прим. ред.*

мые для цифрового профиля физических и юридических лиц, несколько различаются, что определяется их разной ролью и статусом в обществе и государстве.

Цифровой профиль гражданина включает три составляющих: 1) ключевые данные о гражданине (57 типов юридически значимых сведений); 2) ссылки на другие госструктуры, 3) реестр согласий по обработке персональных сведений, предоставленных человеком различным ведомствам и компаниям. Это означает, что сбор информации о человеке станет почти тотальным, охватывая все государственные, негосударственные, общественные и коммерческие организации. Но «бояться этого нечего, если соблюдаешь общепринятые нормы поведения» [Костылева, 2019].

Гражданин будет сам контролировать, какую информацию о себе и кому передавать, может в любое время просмотреть и пересмотреть реестр своих согласий на обработку личных данных. Возможность отозвать согласие на обработку своих данных с целью блокировки их использования – это важная особенность российского цифрового профиля. Хотя определенную информацию в некоторых случаях из цифрового профиля можно получить без согласия человека.

ФНС на базе сведений ЗАГСов создает Федеральный реестр населения, который станет источником данных для цифрового профиля гражданина. Источником становится также любая активность человека в Интернете и соцсетях. Заходя в Интернет с целью посмотреть события дня, найти нужную информацию, заказать товары и услуги или пообщаться с виртуальным сообществом и выплеснуть накопившиеся эмоции в соцсетях, человек оставляет в нем свой цифровой след. И по сохраняющимся цифровым отпечаткам можно узнать о человеке значительно больше, чем он хотел бы. По словам А. Хачуяна (генерального директора компании Tazeros Global Systems, специализирующейся на разработке систем искусственного интеллекта), цифровой профиль конкретного человека на 40% формируется из данных о самом человеке и 60% представляют данные о его окружении [Семенец, 2019]. Но не вся собираемая информация носит открытый характер. К банковским и медицинским данным доступ имеет собственно носитель – владелец и оператор этих данных.

Базовыми источниками сведений для цифрового профиля организаций и индивидуальных предпринимателей являются ОГРН[1] и ИНН. Цифровой профиль организаций количественно и качественно убыстряет и улучшает взаимодействие центра с субъектами Федерации, госструктур между собой, а также с населением и бизнес-сообществом, между предпринимателями и предпринимателей с потребителями. Цифровая система обмена информацией минимизирует бумажный оборот и позволит удешевить услуги, делая их доступнее для потребителя. Принцип работы практически прежний, но убирается ряд этапов и действует цифровая логистика. Теоретически это

[1] Основной государственный номер, присваиваемый при регистрации всем организациям. – *Прим. ред.*

должно снизить расходы и повысить конкурентные преимущества российского бизнеса, а также повысить эффективность сбора налогов.

Первоначально предполагалось создание цифрового профиля по предложенной Ростелекомом схеме, которая оценивалась в 3,1 млрд руб. При этом корпорация брала на себя функции исполнителя / оператора работ. По этому варианту Ростелеком получал следующие конкурентные преимущества: 1) свободный доступ к базе данных клиентов других хозяйствующих субъектов и 2) информацию о своих конкурентах. Отказ от предложения Ростелекома позволил снизить стоимость проекта в 13 раз [Королев, 2019].

Передача статуса оператора цифрового профиля Минкомсвязи привела к резкому сокращению запрашиваемых средств. По новой схеме на формирование цифрового профиля из федерального бюджета выделяется 235 млн руб., в том числе: 1) на модернизацию существующих механизмов в программной архитектуре ЕСИА – 184 млн руб., 2) на создание цифровых профилей и соответствующей инфраструктуры, на разработку алгоритмов и документации по наполнению профилей и верификации данных, а также на создание подсистемы информирования заявителей – 51 млн руб. [Королев, 2019]. Финансирование инфраструктуры цифрового профиля осуществляется из федерального бюджета – коммерческие структуры по соображениям безопасности к этому не допущены.

Оставить систему у Ростелекома означало передать корпорации в монопольное управление национальную информационную базу обо всем населении и хозяйствующих субъектах, что могло разрушить конкурентную среду. Вместе с тем из-за ограниченности государственных финансовых ресурсов министерство вынуждено идти на многократное снижение стоимости проекта. При этом вероятно снижение качества разработок, но это цена за равный доступ всех к информационной системе цифрового профиля. Хотя экономия в ущерб качеству – это ложный путь, и скупой платит дважды. Кроме того, нельзя отставать от мировых тенденций, и надо учитывая быстро бегущее инновационное время.

Мало создать цифровой профиль. Его надо поставить на баланс, выделять средства на поддержку и функционирование. Или добиться самофинансирования, сделав источником дохода для государственного бюджета. В настоящее время предполагается установить бесплатный доступ к цифровому профилю для физических лиц. Для коммерческих структур этот доступ должен быть платным, а тариф можно «привязать» к получаемому доходу.

Цифровой профиль планируется использовать, прежде всего, на финансовом рынке, что позволит снизить стоимость банковских продуктов. Уже с осени 2019 г. банки в России начали рассчитывать показатель долговой нагрузки заемщиков и с учетом профиля клиента определять его кредитоспособность. Подобные меры были приняты в связи со стремлением Центробанка не до-

пустить «разрастания пузыря» на рынке потребительского кредитования. ЦБ России также отобрал 16 банков для тестирования цифрового профиля [НТВ].

Вместе с тем ряд специалистов в области разработки искусственного интеллекта ставит под сомнение эффективность российской системы цифрового профиля. Может быть, в данном случае желания опережают возможности. Возникают проблемы в связи с качеством оцифровывания данных, а также глубиной и широтой оцифровки. Кроме того, например, «умные» счетчики, установленные в квартирах, не могут передавать в автоматическом режиме информацию о потребленных ресурсах в МФЦ, так как для этого еще не создана необходимая инфраструктура. Китаю потребовалось 15 лет для того, чтобы сконцентрировать весь массив данных пограничной службы, учреждений образования, здравоохранения и других ведомств в электронных базах, которые стали основой для создания цифрового профиля и / или системы социального кредита [Семенец, 2019].

Однако следует помнить, что любое новшество, тем более инновационное, с трудом внедряется в жизнь. На начальном этапе эксплуатации всегда выявляются уязвимые / болевые точки. Нужно время и главное – практика применения изделия (программы), чтобы исключить эти слабые места. Необходимо начать использовать систему, чтобы обеспечить ее совершенствование.

Введение цифрового профиля повышает эффективность и результативность государственных услуг и облегчает жизнь человека. Цифровой профиль позволяет автоматически вводить в анкету данные, находящиеся в электронной базе данных, на что требуется в 10–20 раз меньше времени, чем при заполнении бумажной анкеты. К тому же исключается человеческий фактор: ошибки, фальсификация, а также снижаются риски предоставления поддельных документов и число отказов из-за неправильного оформления документов. Цифровой профиль ускоряет процесс поиска нужного решения и увеличивает объемы предоставляемых услуг. Не требуется каждый раз заполнять анкету при обращении за государственной услугой.

Но собранная информация может обернуться и против человека. Поэтому, предупреждают эксперты, следует продумать все нюансы создания цифрового профиля и последствия его использования с учетом исторического опыта и современных реалий, включая и факторы коррупции [Аитов, 2019].

Алгоритмическая обработка больших данных показывает не только то, что произошло, но и все альтернативы развития события. Однако возможны и ошибки. Допущенные ошибки и искажения информации могут нанести непоправимый ущерб как личности, так и организации.

### *Безопасность и защита данных*

Цифровой профиль должен быть надежно защищен от хакеров, кибервзлома и проникновения в личную жизнь человека с целью повлиять на его физическое, умственное и духовное разви-

тие. По этой же причине генетическая паспортизация населения должна носить добровольный характер.

Сложнейшим вопросом является кто, на каком основании, по каким причинам, с какой целью получает доступ к всеобъемлющей цифровой базе данных о каждом гражданине страны, о каждом собственнике, о каждом предпринимателе и компании. Этот вопрос имеет морально-этический характер, и его решение может как укрепить, так и разрушить баланс доверия, которое служит основой неписаного социального контракта между властью и гражданами, властью и предпринимательством.

Концентрация и централизация всей информации о населении и организациях в одной структуре, во-первых, представляет серьезнейшую угрозу демократическому развитию. Во-вторых, создает возможности манипулирования отдельными социальными группами общества. В-третьих, в случае утечки данные могут быть использованы против людей и организаций, нанести их интересам ощутимый ущерб. Информацию из единой базы данных может получить конкурент, мошенник, представители криминальных структур. Спрос на цифровые данные может породить теневой рынок цифровых данных и определенные круги, которые будут поставлять на рынок запрашиваемые данные.

Против такого развития системы цифрового профиля выступают ФСБ и другие силовые структуры. По их мнению, централизация данных на одной площадке повышает риски утечки конфиденциальных сведений о работниках государственных органов, а также может привести к разглашению персональной информации о лицах, находящихся под государственной защитой, и их семьях [Цифровой профиль …, 2019].

Проблема утечки информации не является пустым звуком. Защита может быть взломана извне в результате хакерских атак или нарушена изнутри. Достаточно вспомнить появление на черном рынке базы данных о клиентах Сбербанка. Помимо этих угроз существуют экономическая разведка и промышленный шпионаж, которые могут нанести непоправимый ущерб национальной и экономической безопасности государства и бизнеса. Следует учитывать рост из года в год количества хакерских взломов, за которыми стоят разные группы и государства. В 2019 г. число хакерских атак только на инфраструктуру и государственные объекты в России выросло на 200% [Федуненко, 2019].

Безопасность цифровых систем зависит, прежде всего, от программного обеспечения. В связи с этим в данном случае желательно использовать отечественные разработки, включая накопительные устройства российского производства.

В целом решать проблему цифрового профиля следует, исходя из интересов человека. По мнению специалистов, продуктом цифрового общества является новая этика, которая опирается на

два взаимосвязанных постулата: 1) человек должен иметь доступ к своим данным в цифровом профиле; 2) человек должен разбираться и понимать принципы работы алгоритмов [Семенец, 2019]. К этому следует добавить право человека: 1) контролировать сбор данных о себе, корректировать эти данные и стирать их при необходимости; 2) знать собирателя / оператора своих данных; 3) защищать свою репутацию в случае системной ошибки и / или нарушения кибербезопасности.

Рамками для сдерживания и регулирования развития цифрового сбора данных и их последующей алгоритмизации может стать нормативная правовая база в области защиты персональных данных.

## Заключение

В России насчитывается более 40 слабо интегрированных между собою государственных информационных систем (ГИС). Наряду с федеральным порталом государственных услуг действуют локальные порталы. Данные физических и юридических лиц собираются различными госорганами с разными целями и задачами. Постоянным сбором персональных данных пользователей также регулярно занимаются банки, интернет-компании и соцсети, сотовые операторы и рекламные площадки, агрегаторы такси и туриндустрия. Каждая госструктура и частные организации пользуются собственной моделью сбора, хранения, обработки и анализа собранной информации. В связи с этим стоит задача интегрировать эти потоки информации в одном центре.

В стране пока действует смешанная модель предоставления государственных услуг с постепенным вытеснением бумажных форм электронными. Портал государственных услуг содержит значительное количество данных различных органов власти (финансовых учреждений, силовых структур, Росстата и др.) и успешно справляется с большим объемом информации. Но ряд услуг можно получить только на сайтах отдельных ведомств. Кроме того, нередки сбои из-за «зависания» систем. Поэтому очевидна необходимость единого личного кабинета гражданина.

Логика развития цифрового профиля / электронного паспорта ведет к объединению цифровых систем всех госструктур с подключением к ней цифровых платформ коммерческих организаций, включая банки, сотовых операторов, индустрию отдыха, а также соцсетей. Хотя отсутствие единого стандарта затрудняет объединение всех информационных баз в единую систему.

В итоге может быть собрана абсолютно вся информация о человеке, позволяющая сформировать, в том числе, его морально-психологический портрет. Сомнительно, чтобы в России была создана система социального кредитования, подобная китайской, однако исключать такой вариант нельзя, учитывая историю страны. В то же время интеграция на одной платформе всех электронных ресурсов многократно повышает эффективность системы цифрового профиля.

Наиболее актуальной остается проблема доступа к электронной базе государственных услуг и системе цифрового профиля. Доступ к ним должен регулироваться. При свободном доступе го-

сударственными информационными ресурсами могут воспользоваться в ущерб человеку или предпринимателю.

Система цифрового профиля должна обеспечивать конфиденциальность и целостность юридически значимой информации. Любое ее случайное или преднамеренное искажение наносит вред собственнику или тому, кто делает запрос. Поэтому информационная база цифрового профиля должна быть надежно защищена, и очевидно, что это должны быть отечественные разработки.

## Список литературы

*Аитов Т.* Цифровой профиль гражданина: вопросов больше, чем ответов // Finversia. – 2019. – 28.05. – URL: https://www.finversia.ru/publication/ocenka/tsifrovoi-profil-grazhdanina-voprosov-bolshe-chem-otvetov-58249 (дата обращения 12.03.2020).

*Королев И.* Цифровой профиль граждан подешевел в 13 раз, когда его отобрали у «Ростелекома» // CNews. – 2019. – 06.08. – URL: https://www.cnews.ru/news/top/2019-08-06_tsifrovoj_profil_grazhdan_podeshevel_v_13_razkogda (дата обращения 12.03.2020).

*Костылева Т.* Цифровой профиль гражданина – что известно на сегодняшний день. // D-Russia.ru. – 2019. – 27.03. – URL: http://d-russia.ru/tsifrovoj-profil-grazhdanina-chto-izvestno-na-segodnyashnij-den.html (дата обращения 12.03.2020).

*Леонидов С.* Скоринг во времена «Большого брата»: как банки будут выдавать кредиты к 2020 году // Forbes Contributor. – 2017. – 12.05. – URL: https://www.forbes.ru/tehnologii/342269-skoring-vo-vremena-bolshogo-brata-kak-banki-budut-vydavat-kredity-k-2020-godu (дата обращения 12.03.2020).

*Литвиненко Ю.* Facebook раскрыл данные о «слежке» за пользователями // Ведомости. – 2020. – 28.01. – URL: https://www.vedomosti.ru/technology/articles/2020/01/28/821653-facebook-slezhke (дата обращения 12.03.2020).

Может ли ваш цифровой профиль сработать против вас? // Executive.ru. – 2019. – 14.06. – URL: https://www.e-xecutive.ru/finance/novosti-ekonomiki/1990700-mozhet-li-vash-tsifrovoi-profil-srabotat-protiv-vas (дата обращения 12.03.2020).

НТВ. Цифровой профиль россиянина: ответы на главные вопросы // НТВ. – URL: https://www.ntv.ru/cards/2941/ (дата обращения 12.03.2020).

Самые большие социальные сети в мире. Лучшие социальные сети // CDDISKI.RU. – 2019. – URL: https://cddiski.ru/samye-bolshie-socialnye-seti-v-mire-luchshie-socialnye-seti.html (дата обращения 12.03.2020).

*Семенец А.* Цифровой след приведет к любому // Росбалт. – 2019. – 22.05. – URL: https://www.rosbalt.ru/moscow/2019/05/22/1782565.html (дата обращения 12.03.2020).

*Федуненко Е.* Хакеры нацелились на инфраструктуру. Количество кибератак выросло в три раза // КомерсантЪ. – 2019. – 06.08. – URL: https://www.kommersant.ru/doc/4053350 (дата обращения 12.03.2020).

Цифровой профиль российского гражданина может стать удобной мишенью для хакеров // КомерсантЪ. – 2019. – 13.11. – URL: http://www.iksmedia.ru/news/5623672-Czifrovoj-profil-rossijskogo-grazhd.html (дата обращения 12.03.2020).

# УМНЫЕ УСТРОЙСТВА, КИБЕРСТРАХОВАНИЕ И УТЕЧКИ ДАННЫХ: НОВЫЕ ПРОБЛЕМЫ И НОВЫЕ РЕШЕНИЯ

**Иванова Ангелина Петровна**

Старший лаборант Отдела правоведения Института научной информации по общественным наукам РАН (ИНИОН РАН), (Москва, Россия)

***Аннотация.*** *Практически повсеместные в настоящее время контакты людей с «умными» устройствами подвергают персональные данные пользователей множеству новых угроз. Для того чтобы справиться с информационными рисками, компании начали приобретать полисы киберстрахования. Помимо этого, представляется целесообразным введение уникального индивидуального идентификатора на основе технологии блокчейн и / или биометрических данных.*

***Ключевые слова:*** *Интернет вещей; информационная безопасность; персональные данные; киберстрахование; блокчейн.*

**Для цитирования:** Иванова А.П. Умные устройства, киберстрахование и утечки данных: новые проблемы и новые решения // Социальные новации и социальные науки. – Москва: ИНИОН РАН, 2020. – № 1. – С. 143–148.

URL: https://sns-journal.ru/ DOI: 10.31249/snsn/2020.01.11

## Введение

На сегодняшний день почти вся жизнь людей проходит во взаимодействии с интеллектуальными устройствами. Цифровизация создает особый взаимосвязанный мир, в котором люди подключены к Интернету вещей, включающему в себя «умные» телевизоры, термостаты, мобильные телефоны, автомобили и даже промышленные системы управления. Интеллектуальные помощники, такие как Siri, Google Now и другие, не отключаются никогда, реагируя в любое время на голосовые команды, например, «Okay, Google» [Privacy and liberty …, 2017, p. 36]. Однако вместе с удобствами гаджеты привносят в нашу жизнь и новые угрозы – угрозы кибербезопасности. Увеличивается опасность кибератак, которые могут иметь различные формы в зависимости от цели их совершения.

## Информационная безопасность

В целом понятие «Интернет вещей» довольно неоднозначно и различается в зависимости от того, какой ученый или правительственное учреждение дает ему определение. Один из подходов представляет Интернет вещей как «расширение глобальной инфраструктуры за счет развивающихся информационно-коммуникационных технологий, которые включают в себя взаимосвязь физических и виртуальных систем с другими системами» [DiGrazia, 2018, p. 257]. И хотя большинство людей слышали об Интернете вещей, не все из них понимают, как он влияет на них. Многие потребители могут вовсе не осознавать объем данных, собираемый их устройствами. В большинстве случаев они не знают, какие возможности есть у постоянно активных девайсов. В то время как эти устройства являются частью Интернета вещей и могут быть каналом для проникновения хакеров в дома своих владельцев.

Угроза раскрытия личной информации становится все более реальной в жизни современного общества. В сентябре 2017 г. бюро кредитных историй Equifax объявило, что его база данных была взломана. В результате этого под угрозу была поставлена конфиденциальная информация примерно 143 млн американских потребителей, что составляет около 44% населения. Хакеры смогли получить доступ к «именам людей, социальным сетям, номерам социального страхования, датам рождения, адресам, и, в некоторых случаях, номерам водительских удостоверений» [Marcus, 2018, p. 556]. В результате атаки вируса-шифровальщика WannaCry хакеры смогли за несколько дней взломать более 300 тыс. компьютеров более чем в 150 странах мира, включая компьютеры многих больниц, которые лишились доступа к медицинским записям пациентов. Вирус использовал уяз-

вимости операционной системы Microsoft Windows и шифровал файлы в компьютерах до тех пор, пока пользователь не платил «выкуп» [DiGrazia, 2018, p. 269].

Эти два инцидента иллюстрируют потенциал катастрофического воздействия, которое один хакер может оказать на миллионы людей по всему миру. Основными целями субъектов киберпреступлений являются банковские и валютно-обменные платформы. По официальным данным, в 2015 г. в результате киберкраж было похищено более 300 млн долл. Однако, по оценкам компании «Лаборатория Касперского», специализирующейся в области компьютерной безопасности, реально эта сумма может быть в три раза больше [DiGrazia, 2018, p. 268].

Первостепенное значение для обеспечения национальной безопасности имеет отражение кибератак на автоматизированные системы управления, которые рассматриваются в качестве одной из самых больших угроз. Автоматизированные системы управления обычно определяются как «различные типы систем управления и связанных с ними контрольно-измерительных приборов, которые включают в себя устройства, системы, сети и средства управления, используемые для автоматизации производственных процессов» [DiGrazia, 2018, p. 270]. В настоящее время они применяются практически во всех сферах человеческой деятельности, от сферы общественного питания до фармацевтики. В 2014 г. хакеры продемонстрировали, что имеют возможность получить доступ к автоматизированным системам. Так, была взломана система немецкого сталелитейного завода, а также система управления дамбой в северной части штата Нью-Йорк [DiGrazia, 2018, p. 271].

Согласно отчету страховой компании Lloyd Emerging Risk за 2015 г., кибератака на энергосистему США может обойтись национальной экономике в более чем 1 трлн долл и более чем 70 млрд долл – для страховых компаний. Основная проблема киберрисков (которая не была отражена в данном отчете) заключается в том, что они не ограничены физическими границами и могут причинить огромный вред при минимальных затратах со стороны хакера – достаточно всего нескольких строк вредоносного кода [DiGrazia, 2018, p. 267].

Причин успешности кибератак множество. Главная из них – недостаток знаний о том, как управлять кибербезопасностью (неосведомленность о методах борьбы с манипулятивной деятельностью или отсутствие соответствующих навыков правоприменения), что приводит к недостатку внимания, уделяемого этим вопросам.

## Способы противостояния киберугрозам

По данным страховой компании Allianz, киберпреступность обходится мировой экономике в 445 млрд долл. в год [DiGrazia, 2018, p. 261]. Для того чтобы справиться с киберрисками, многие компании начали приобретать полисы *киберстрахования*.

Страхование помогает частным лицам и компаниям справиться с неизбежными и постоянными рисками. Полисы киберстархования – это относительно новый страховой продукт, предназначенный для освобождения застрахованного лица от расходов, связанных с хакерством, кибератаками и утечками данных. Они обычно подразделяются на две основные категории: страхование «первой» и «третьей» стороны. Первое подразумевает покрытие расходов на уведомления о нарушении конфиденциальности данных, кредитный мониторинг, операционные расходы, смягчение репутационного ущерба. Второе включает покрытие расходов, связанных с привлечением к ответственности (штрафы, мировые соглашения и т.д.).

Необходимость киберстрахования в последнее время стала предметом многочисленных дискуссий. Некоторые считают, что суммы денежных средств, которые компании платят в качестве страховых премий, сопоставимы с суммами, которые они вынуждены заплатить для устранения последствий кибератак и утечек данных. Более того, компании, возможно, могли бы предотвратить кибератаки, если бы использовали деньги, потраченные на киберстрахование, для укрепления защиты своих информационных сетей [DiGrazia, 2018, p. 260]. Другие считают, что киберстрахование является хорошей инвестицией для малого и среднего бизнеса, который может серьезно пострадать от кибератак, но не имеет финансовых возможностей для проведения аудита IT-рисков и предотвращения кибервторжений.

На самом деле, малый и средний бизнес стали главной мишенью для хакеров, потому что не имеют опыта или средств, которыми располагают крупные компании для защиты своих сетей. Киберстрахование может быть ценным вложением и для крупных компаний, которые имеют дело с большим количеством данных, таких как организации розничной торговли, медицинские организации, финансовые компании и т.д. При этом фирмы, приобретающие киберстраховки, должны понимать, какие расходы будут покрывать их страховые полисы, а какие могут дублировать страховые покрытия, и какие риски остались незастрахованы.

Например, в США большинство действующих полисов страхования гражданской ответственности основаны на стандартных формах, разработанных Управлением в сфере страхования (Insurance Service Office – ISO). Современные полисы охватывают три области расходов: имущественная ответственность и ответственность за причинение вреда здоровью; ответственность за нарушения в сфере рекламы; медицинские выплаты. Несмотря на то что сфера киберстрахования является относительно новой, базовые элементы страховых полисов неоднократно пересматривались страховыми компаниями и судами. Ввиду этого ISO определило, что раз в несколько лет необходимо менять стандартные формы полисов.

Модели потерь, используемые страховыми компаниями для таких полисов, как страхование автомобилей, страхование жизни и страхование жилых помещений, позволяют предсказать ожи-

даемый убыток на основе агрегирования большого числа независимых рисков, неоднократно повторяющихся в течение длительного периода времени. В настоящее время страховые компании разработали сложные инструменты моделирования и, как правило, имеют возможность предвидеть убытки, связанные со стихийными бедствиями. Хотя в 2005 г. некоторые из них были застигнуты врасплох и понесли серьезные убытки в результате урагана «Катрин». Вместе с тем потери от крупного инцидента в цифровом мире, например потери от утечки данных, могут не быть локализованы на территории одной стороны, что делает такие инциденты гораздо опаснее для страховых компаний [DiGrazia, 2018, p. 269].

Пример вируса WannaCry продемонстрировал, что даже при наличии надежного рынка перестрахования масштабная кибератака может привести к банкротству как первичных страховых компаний, выпускающих полисы, так и перестраховщиков. Это происходит потому, что страховые компании пытаются выпускать полисы для покрытия угроз, создаваемых людьми, которые, как правило, трудно моделировать и страховать.

Используемая в киберпреступлениях уязвимость провоцирует массовый каскадный эффект, приводящий к триллионам застрахованных убытков. В результате возникают значительные проблемы у страховых компаний, которые оформляют полисы киберстрахования. Хакерские действия могут вызвать цепь событий, влекущих за собой выплату страхового возмещения по разным видам страхования: киберстрахованию, страхованию жилых помещений и даже полисам автострахования. Вероятность массовых правонарушений, связанных, например, с использованием номеров социального страхования в США, ставит под угрозу компании, хранящие эти данные. Отрицательные последствия имеют место и для потребителей: им приходится тратить значительные средства на оплату постоянного кредитного мониторинга, предотвращение рисков кражи личных данных и возможность быстрого замораживания счетов.

Диверсификация рисков на рынке киберстрахования потребовала углубленного сценарного анализа потенциальных рисков, связанных с киберпреступлениями. Как выяснилось, действующие в настоящее время страховые полисы не соответствуют миру с Интернетом вещей. Ввиду несовершенства существующих методов идентификации отдельных лиц в гражданском обороте высказывается мнение о необходимости перейти к альтернативным способам.

Одним из наиболее популярных вариантов, предлагаемых экспертами по обеспечению безопасности, является *использование многофакторной биометрии* для идентификации человека, такой как распознавание голоса / лица, сканирование радужной оболочки и т.д. Другая альтернатива – это *применение технологии блокчейн*, которая позволяет создать «публичный регистр транзакций» [DiGrazia, 2018, p. 272].

Технология блокчейн уже применяется Эстонией в качестве основы для цифровой идентификационной системы в сфере медицинских услуг, на контрольно-пропускных пунктах, а также для голосования на выборах. Такие компании, как IBM и SecureKey, используют блокчейн при разработке идентификационных решений, основанных на «ориентированной на пользователя модели, также известной как суверенная идентичность», которая позволяет пользователям контролировать количество лиц, имеющих доступ к их личной информации [DiGrazia, 2018, p. 276].

Переход на систему идентификации на основе блокчейн, возможно, был бы оптимальным решением для стран с большой численностью населения, поскольку она не требует от правительства сбора биометрических данных граждан, но позволяет предотвратить мошеннические транзакции. Преимущество использования алгоритмов блокчейн заключается также в том, что по мере совершенствования технологий взлома алгоритмы могут совершенствоваться вместе с ними.

Одним из наиболее значимых препятствий на пути внедрения блокчейн-технологий является опасение, что цифровые записи будут умышленно изменены или уничтожены. Однако данный аргумент носит спорный характер, поскольку зашифрованный публичный реестр, в котором хранятся данные, технически не может быть уничтожен или переписан.

## Заключение

Благодаря Интернету вещей возник мир, где почти все, что делают люди, зависит от информации и взаимосвязанных компьютерных систем. При этом растущее количество и масштабы кибератак свидетельствуют о значительности ущерба, к которому приводят инциденты в цифровой сфере. Вместе с тем в настоящее время существуют и меры, которые государства, бизнес и физические лица могут предпринять для своей защиты.

Во-первых, компании могут использовать альтернативный уникальный идентификатор пользователей на основе технологии блокчейн и / или биометрических данных. Во-вторых, страховые компании могут стимулировать организации к повышению уровня безопасности данных, предлагая более выгодные тарифы тем, кто внедряет более надежные механизмы защиты. Однако следует помнить о массовом каскадном эффекте, которым обладают инциденты в цифровой сфере ввиду высокого уровня ее взаимосвязанности.

## Список литературы

*DiGrazia K.* Cyber Insurance, Data Security, and Blockchain in the Wake of the Equifax Breach // Journal of Business & Technology Law. – Baltimore, 2018. – Vol. 13, N 2. – P. 255–277.

*Marcus D.J.* The data breach dilemma: proacrtive solutions for proptecting consumers' personal information // Duke law journal. – Durham, NC, 2018. – Vol. 68, N 555. – P. 555–593.

Privacy and liberty in an alaways-on, always-listening world / Bohm A.S. and other // The Columbia science and technology law review. – New York, 2017. – Vol. 19, N 1. – P. 1–45.

# КИБЕРБУЛЛИНГ:
# ПРИЧИНЫ ЯВЛЕНИЯ И МЕТОДЫ ПРЕДУПРЕЖДЕНИЯ


**Коданева Светлана Игоревна**

Кандидат юридических наук, старший научный сотрудник Отдела правоведения Института научной информации по общественным наукам РАН (ИНИОН РАН), (Москва, Россия)



***Аннотация***. *Цифровые технологии стали неотъемлемой частью нашей жизни, открывая новые возможности, но в то же время вызывая и новые риски. Одним из негативных явлений, приобретающим все большее распространение по всему миру, стало формирование агрессивной среды в социальных сетях и на сетевых платформах, где молодежь проводит значительную часть своего времени. Эта среда порождает такое явление, как кибербуллинг – умышленное причинение психического вреда жертве, не способной себя защитить. В настоящем исследовании представлен анализ факторов, провоцирующих детей и подростков на проявление агрессии по отношению к своим сверстникам в виртуальном мире, а также сформулированы предложения по предупреждению этого опасного явления.*



***Ключевые слова:*** *цифровая среда; кибербуллинг; киберагрессия; цифровая безопасность.*

**Для цитирования:** Коданева С.И. Кибербуллинг: причины явления и методы предупреждения // Социальные новации и социальные науки. – Москва: ИНИОН РАН, 2020. – № 1. – С. 149–159.

URL: https://sns-journal.ru/ DOI: 10.31249/snsn/2020.01.12

## Введение

Появление Интернета кардинально изменило нашу повседневную жизнь, наполнив ее онлайн-сервисами, приложениями и общением. Для многих людей виртуальная среда стала не менее значимой, чем реальный мир. Причем влияние Интернета с течением времени усиливается, принося не только удобства, но и опасности, связанные с ростом киберпреступности.

Онлайновая виктимизация[1] может проявляться в разных формах. К числу наиболее обсуждаемых относится кража личных данных, мошенничество, финансовые преступления. В то же время молодежь и дети, получившие легкий доступ в виртуальный мир и зачастую не подготовленные к различным рискам, могут стать жертвами чудовищных преступлений в Интернете, таких, как детская порнография или торговля людьми в сексуальных целях. Но даже если не принимать во внимание все откровенно преступные цели использования Сети, молодое поколение все чаще сталкивается здесь с проблемой запугивания и преследования со стороны своих ровесников, так называемым кибербуллингом.

В киберпространстве люди чувствуют себя более раскованными в эмоциях, словах и поведении. Одновременно они становятся все более зависимыми от виртуальной среды – здесь проще знакомиться и общаться, раскрывая свое истинное «я». В социальных сетях и блогах можно говорить и делать то, что сложно сделать в физическом мире, включая издевательства и оскорбления. В результате формируется специфическая, прежде всего молодежная, культура, где такое поведение считается приемлемым или, по крайней мере, ожидаемым. В Интернете постоянно появляются новые методы запугивания и преследования – в новых приложениях или на новых интернет-форумах, – что затрудняет борьбу с этим развивающимся негативным явлением. По данным последних исследований, почти половина подростков (49%) совершали агрессивные действия в Интернете, и более половины (61%) подвергались киберагрессии [Calpbinici, Arslan, 2019].

Как отмечала в 2010 г Всемирная организация здравоохранения (ВОЗ), кибербуллинг является серьезной проблемой общественного здравоохранения, влияя на психическое и физическое здоровье детей и подростков во всем мире. По данным ВОЗ 2017 г., депрессия является третьей ведущей причиной болезней и инвалидности среди подростков, а самоубийство – третьей причиной преждевременной смерти в этой возрастной группе [Calpbinici, Arslan, 2019]. Особенно сильно эти

[1] Виктимизация (лат. victima – жертва) – процесс или конечный результат превращения в жертву преступного посягательства.

мучительные и навязчивые формы поведения проявляются в возрасте 12–18 лет, когда происходит процесс социализации.

Безусловно, проблема подавления и запугивания одних детей и подростков другими, особенно в школе, а затем в армии (известная в России как дедовщина) – это не новое явление. Оно достаточно хорошо изучено психологами, характеризующими его как постоянное воздействие на одного ребенка физической и / или эмоциональной агрессии (включая поддразнивание, обзывательство, насмешки, угрозы, притеснения, издевательства, дедовщину, социальное отчуждение и слухи), осуществляемое в течение длительного времени и с намерением причинить вред. Поэтому многие исследователи рассматривают кибербуллинг как очередное проявление традиционного запугивания [например, Herrera-López, Romera, Ortega-Ruiz, 2017; Cyberbullying and traditional bullying ..., 2017; Latent class analysis …, 2019; The differential victimization ..., 2019]. Однако нельзя полностью согласиться с таким подходом.

Представляется, что это все-таки два разных типа издевательств. Традиционные издевательства часто происходят в школе и связаны с проблемой лидерства в конкретно взятой социальной группе. При этом ребенок, покидая школу, может вступать в иные социальные отношения. Напротив, кибербуллинг может происходить в любое время дня и ночи без ограничений. В реальном мире запугивание происходит в таких формах как физическое, вербальное и реляционное запугивание. Кибербуллинг в основном направлен на чувства жертвы и ее социальные отношения. При этом могут использоваться совершенно иные приемы, такие как размещение в социальных сетях порочащих фотографий, видеороликов, вербальных издевательств с использованием специфической терминологии или смайликов. Принципиально иным является и дисбаланс власти в традиционных издевательствах и кибербуллинге. Обычное запугивание, как правило, связано с физическим превосходством ученика или группы, претендующих на доминирующее положение в классе (школе). В случае кибербуллинга это совершенно не обязательно. Человек, страдающий физическими недостатками, может их компенсировать агрессивным поведением и травлей в отношении эмоционально слабых или зависимых жертв.

## Кибербуллинг как социальное явление: понятие и основные черты

Существует много типов кибербуллинга, которые различаются в зависимости от намерений, продолжительности и оказываемого на жертву воздействия. Можно выделить следующие специфические особенности кибербуллинга, отличающие его от традиционного издевательства.

Во-первых, в виртуальном пространстве агрессивная сторона не может непосредственно наблюдать реакцию своей жертвы. В результате, с одной стороны, она не опасается ответной реакции, как при прямом контакте в реальном мире; проявляет меньше сочувствия к жертве; чувство вины или угрызения совести ослабевают или исчезают полностью. С другой стороны, хулиган не

получает такого же морального удовлетворения, как от прямой агрессии. Таким образом, мотивация в случае обычного запугивания или издевательства и кибербуллинга может существенно различаться [Bullying in the digital age ..., 2014; Bauman, 2009; Runions, Bak, 2015].

Исследования, посвященные избирательному моральному отчуждению (т.е. когнитивному процессу, с помощью которого человек оправдывает свое собственное вредное или агрессивное поведение по отношению к другим путем ослабления внутренних саморегуляторных механизмов), показывают, что люди легче причиняют вред другим, когда этот вред невидим для преступников благодаря расстоянию либо времени [Mechanisms of moral disengagement …, 1996]. Представляется, что данные выводы полностью коррелируют с отношениями в цифровой среде, создающей благоприятную атмосферу для морального отчуждения, антисоциального поведения и проявления установок, противоречащих общественным нормам.

Во-вторых, подразумеваемая при онлайн-общении анонимность позволяет делать или говорить вещи, которые человек не осмелился бы сделать или сказать в личных отношениях. Поэтому язык, используемый в Интернете, часто более эмоционален и жесток.

Ряд исследований подтверждают, что анонимность создает эффект «растормаживания», который часто является катализатором кибератак. По предположению специалистов, эффекту растормаживания в Интернете способствуют следующие условия цифровой среды: диссоциативная анонимность («они никогда не узнают, кто я на самом деле»); невидимость («я не могу видеть тебя, поэтому ты не можешь видеть меня»); асинхронность («я выложу все, что хочу сейчас, и ты увидишь это позже, когда мне не придется иметь дело с твоей реакцией»); диссоциативное воображение («тот, кто я есть в Сети, отличается от того, кто я есть в реальной жизни»), а также минимизация авторитета («нет никаких последствий для того, что я говорю или делаю в Сети») [Suler, 2004].

В-третьих, число случайных свидетелей при кибербуллинге значительно больше, чем при традиционных издевательствах. Проведенные исследования доказали, что случайные свидетели играют очень большую роль в случае кибербуллинга [The differential victimization ..., 2019]. При этом в цифровой среде отсутствуют важные социальные сигналы, которые могли бы сдерживать подобное поведение, поскольку свидетели воспринимают ситуацию как должное и не «одергивают» хулигана, как это бывает в реальном мире. Еще одна особенность заключается в том, что преступники, жертвы и свидетели могут получить доступ к контенту в любое время (24 часа в сутки, семь дней в неделю) [Student bystander behaviour ..., 2016].

Таким образом, под кибербуллингом понимают агрессивные, преднамеренные действия, осуществляемые неоднократно и / или в течение долгого времени группой или отдельным лицом с использованием компьютеров, мобильных телефонов и электронных устройств против жертвы,

которая не может защитить себя [Marcum, Higgins, 2019; The differential victimization ..., 2019]. Хотя даже однократное действие может рассматриваться как кибербуллинг, если его последствия длятся в течение долгого времени. Например, один неприятный слух, опубликованный на странице в социальных сетях, может быть неоднократно перепостирован (растиражирован).

Кибербуллинг может осуществляться в разных формах: эмоциональное разжигание (emotional flaming – онлайн-драка), онлайн-издевательства (online harassment – повторяющиеся оскорбления или насмешки), онлайн-ненависть (online hate – враждебное и оскорбительное взаимодействие), киберпреследования (cyber-stalking – онлайн-мониторинг партнера для определения, где он находится или с кем он находится в настоящее время, либо отправка жертве повторяющихся угроз), очернение (denigration – размещение недостоверной информации), маскарад (masquerade – создание поддельных профилей для размещения ложной или вредной информации), самозванство (impersonation – размещение постов в социальных сетях от имени жертвы), вымогательство (outing – вымогательство личной информации у кого-то, а затем электронный обмен этой информацией с другими), секстинг (sexting – распространение интимных фотографий другого человека без его согласия) и онлайн-отчуждение (online exclusion – удаление из друзей или блокировка) [The «net» of the internet …, 2016; Online hate ..., 2016; Livazovic, Ham, 2019].

Киберагрессии имеют разнообразные негативные последствия. Многочисленные исследования выявили сильное влияние на здоровье людей различных форм издевательств, причем не только жертв, но и самих хулиганов. Так, жертвы склонны к развитию депрессии и тревожности, суицидальным мыслям. Они становятся замкнутыми, не обращаются за помощью и чувствуют себя все более и более беспомощными. Это приводит к снижению успеваемости в школе и самооценки личности, негативно влияет на физическое здоровье (учащенное сердцебиение, боли в желудке, потливость или головокружение). Может появиться бессонница, раздражительность или вспышки гнева, деструктивное и агрессивное поведение, трудности с концентрацией внимания, повышенное чувство опасности для себя или других, а также нервозность или испуг от чего-то неожиданного [Baldry, Sorrentino, Farrington, 2019; Garaigordobil, Machimbarrena, 2019; Cyberbullying in gifted students ..., 2019]. Все перечисленное – это симптомы посттравматического стресса. Кибербуллинг также оказывает влияние на общие аспекты субъективного благополучия, такие как удовлетворенность жизнью или счастье [Moore, Huebner, Hills, 2012; The impact of cyberbullying ..., 2013]. Кроме того, издевательства в подростковом возрасте могут выступать фактором вовлечения в различные аддиктивные[1] формы поведения, такие как потребление наркотиков [Cyberbullying,

[1] Аддиктивное поведение (от англ. addiction – склонность, пагубная привычка; лат. addictus – рабски преданный) – особый тип деструктивного поведения, которое выражается в стремлении к уходу от реальности посредством специального изменения своего психического состояния.

school bullying ..., 2012], алкоголя [Chan, La Greca, Peugh, 2019], пристрастие к азартным играм [The relationship between ..., 2019].

В свою очередь, лица, ведущие себя агрессивно в киберпространстве, тоже страдают от различных расстройств здоровья. В частности, они проявляют симптомы депрессии и тревоги [Do cyberbullies suffer ..., 2013], деструктивного поведения [Cyberbullying, problematic internet use ..., 2014], снижения успеваемости в школе [Wright, 2015] и повышения уровня стресса [Informe Ejecutivo ..., 2017]. Кибер-хулиганы также подвергаются повышенному риску суицидального поведения и снижения субъективного благополучия по сравнению с не вовлеченной в кибербуллинг молодежью [Friendship quality ..., 2019].

Следует отметить, что установленным фактом является сочетание в одной личности ролей агрессора и жертвы [Akbulut, Eristi, 2011; Del Rey, Elipe, Ortega-Ruiz, 2012; Gordillo, Antelo, Martín-Mora, 2019; Kokkinos, Antoniadou, 2019]. Исследователи обнаружили, что кибервиктимизация была важным фактором для вовлечения молодых людей в кибербуллинг в роли агрессора. Вероятность того, что подросток станет киберхулиганом, у жертв кибербуллинга увеличивалась в 15 раз [Health-related risks ..., 2019]. Это также является характерной особенностью киберагрессии. В реальном мире, как правило, издевательства совершаются теми, кто обладает большей физической силой, вербальными или социальными навыками, а их жертвы не могут отомстить или «отыграться» на других. Однако в Интернете такие недостатки могут быть скрыты или даже компенсированы, когда жертва насилия сама начинает проявлять агрессию, издеваясь или унижая других пользователей Сети. Соответственно, киберагрессия может быть обусловлена ситуационными факторами, такими как провокация.

Очевидно, что кибербуллинг – это явление, принципиально отличное от обычных запугивания и издевательств. Оно несет множество крайне негативных последствий для всех участников (жертвы, хулигана и свидетелей), которые могут проявляться в течение всей последующей жизни. Это обусловливает важность и актуальность изучения мотивов, лежащих в основе развивающейся культуры кибервраждебности, и выработки адекватных механизмов противодействия ей.

## Причины кибербуллинга

К настоящему времени проведено довольно много различных исследований, каждое из которых концентрируется на тех или иных причинах киберагрессии. При этом они не рассматривают кибербуллинг комплексно, с учетом как личностных факторов, так и факторов окружающей среды. Большинство ученых связывают кибербуллинг с характеристиками личности жертвы и хулигана. Подчеркивается, что социальные сети привлекают социально озабоченных людей и тех, кто не может заниматься офлайн-хулиганством. Кибербуллинг называют «идеальным преступлением» из-за легкости его совершения и минимальных последствий для преступника [Englander, 2008].

Действительно, Интернет представляет привлекательную альтернативу для людей, которые эмоционально изолированы, социально отчуждены или чрезмерно застенчивы. Одиночество, выражающееся в отсутствии друзей, трудностях в установлении близких отношений, низком интересе к социальной активности, заставляет таких людей больше времени проводить в Сети [Nowland, Talbot, Qualter, 2018]. Подобное поведение трактуется как «воспринимаемая социальная изоляция», которая способствует развитию склонности совершать или быть мишенью кибербуллинга [Cacioppo, Hawkley, Thisted, 2010].

Социальные сети позволяют, обеспечивая анонимность, полностью проявить все черты личности, которые принято скрывать в обычных отношениях. Подростки, обладающие признаками нарциссизма, психопатии или садизма, демонстрируют повышенную сетевую расторможенность, что признается прямым предиктором кибератаки [Kureka, Josea, Stuartb, 2019]. К кибербуллингу также склонны люди, у которых агрессия является постоянной чертой характера, включая враждебность к окружающим, гневливость и раздражительность [Which personality traits ..., 2017; Savage, Tokunaga, 2017].

Основными факторами риска вовлеченности в кибербуллинг как в качестве киберхулигана, так и в качестве жертвы считаются употребление психоактивных веществ, низкая самооценка и проблемы психического здоровья, низкая религиозность и депрессивные симптомы. К ним также относится интернет-зависимость (пользование Интернетом более трех часов в день, раскрытие большого объема личной информации) в сочетании с низким уровнем технических навыков, когда ребенок или подросток сообщает пароли от своих профилей и страниц друзьям, позволяет им загружать различный контент.

Имеют значение и условия окружающей среды, постоянно влияющие на личность индивида [Peter, Petermann, 2018]. Так, побудить к сетевой агрессии могут конфликтные семейные отношения; принадлежность к расовому, этническому, культурному или религиозному меньшинству; отсутствие социальной поддержки; влияние средств массовой информации, пропагандирующих насилие и препятствующих развитию критического мышления; онлайн- и видеоигры [Zych, Ortega-Ruiz, Marin-Lopez, 2016; Tudkuea, Laeheem, Sittichai, 2019; Cortés, De los Ríos, Pérez, 2019]. Кроме того, важную роль в кибербуллинге играет атмосфера на соответствующей платформе. Если в конкретном интернет-сообществе не поощряется агрессивное поведение, то это может стать сдерживающим фактором даже для психологически предрасположенных к кибербуллингу людей. Напротив, иррациональная атмосфера ненависти, базирующаяся на субъективных эмоциональных комментариях, будет поощрять агрессивных людей к кибербуллингу.

Самое худшее заключается в том, что кибертравля – это больше, чем просто отдельные инциденты. Она формирует поведенческие паттерны, которые со временем могут становиться все

более жестокими, если не будут пресекаться родителями, образовательными учреждениями и государственными органами. Поскольку складывающиеся образцы поведения в виртуальной среде начинают восприниматься в качестве общей социальной нормы, то расширение кибербуллинга оказывает разрушительное воздействие на молодежь.

## Возможности противодействия

Исследование причин, способствующих появлению и развитию кибербуллинга, позволяет сделать вывод, что это принципиально новое социальное явление. Оно обусловлено, прежде всего, стремительным развитием цифровых технологий и неготовностью детей и подростков к здоровому взаимодействию и общению в виртуальной среде, формирующей собственные образцы поведения. При этом фундаментом новых социальных моделей являются особенности эмоционального и психического состояния личности, т.е. те стороны, которые в реальном мире глубоко скрыты от окружающих. Поэтому традиционные меры борьбы с кибербуллингом как с разновидностью обычного хулиганства оказываются неэффективными.

Дети, вовлеченные в киберагрессию, редко делятся своими проблемами с родителями или учителями. Представители правоохранительных органов, в свою очередь, могут восприниматься жертвами киберпреступлений с недоверием и даже враждебно. С учетом анонимности, которую предоставляет Интернет, достаточно трудно выявить реальных киберхулиганов, собрать доказательства их преступной деятельности и привлечь к ответственности.

Неудивительно, что все большее число исследователей приходят к выводу, что ключевое значение для защиты молодых людей, попавших в ситуацию киберагрессии, имеет повышение их психологической устойчивости [Hinduja, Patchin, 2017; Przybylski, Bowes, 2017]. Важно учить детей и подростков эффективным и ориентированным на решение задач стратегиям поведения: преодоление негативных жизненных ситуаций, которых невозможно избежать, вместо затаивания, приводящего либо к повышенной агрессии в Сети, либо к интернет-зависимости и раскрытию личной информации, что часто делает ребенка жертвой кибербуллинга. Кроме того, необходима разработка специальных образовательных программ, обучающих правильному поведению в Интернете, включая информирование о последствиях размещения личных данных, фотографий и видео в открытом доступе, а также о признаках нездорового поведения.

Но, пожалуй, самое важное – это формирование морального неприятия кибернасилия у свидетелей подобных инцидентов. Люди, находящиеся в непосредственном окружении жертв и / или киберхулиганов, играют решающую роль в выявлении и предотвращении этих действий. На платформах, где большинство пользователей осознают опасность кибербуллинга и бойкотирует его, распространение кибернасилия в конечном итоге прекращается независимо от первоначальных

активных действий киберхулиганов и людей, которые комментируют или постят соответствующий контент [Wagner, 2019; Spreading dynamics ..., 2019].

Таким образом, очевидна необходимость повышения грамотности пользователей Сети в вопросах кибернасилия и в знании законодательства, запрещающего подобные действия, а также осознания ими своей ответственности за окружающих людей и необходимости защиты жертв киберагрессии. Следует подчеркнуть и важный сдерживающий эффект культуры. В обществах, в которых культивируются коллективистские ценности, кибербуллинг менее распространен, чем в обществах с преобладанием индивидуалистических ценностей.

## Заключение

Нельзя не признать, что кибербуллинг – это крайне негативное и опасное социальное явление. Он распространяется все шире по мере развития цифровых технологий, затрагивая все большее число детей и подростков во всем мире. В связи с этим крайне актуальным является определение причин, провоцирующих киберхулиганов к агрессии и легко превращающих многих людей в жертвы такого рода преступлений. Следует как можно скорее разработать комплексные программы противодействия кибернасилию, которые должны включать как соответствующее обучение родителей и педагогов, так и проведение психологических тренингов с детьми и подростками. Людей нужно научить правилам безопасного поведения в Сети и навыкам противодействия кибербуллингу.

Но самое главное – необходимо повысить роль культурного воспитания детей, прививая им нетерпимость к агрессии и готовность поддержать жертву насилия. Стоит прислушаться к ученым, которые в последнее время все активнее призывают более критично относиться к экспансии слишком либеральных (толерантных к девиантному поведению) взглядов. В эпоху глобализации и цифровизации все большее число государств понимает важность сохранения традиционной общественной морали и ценностей.

Российской культуре всегда были свойственны коллективистские ценности, сострадание и сопереживание ближнему, стремление защитить того, кто слабее. Опора на эти традиции помогает бороться с негативными сторонами цифрового общества.

## Список литературы

*Akbulut Y., Eristi B.* Cyberbullying and victimisation among Turkish University students // Australasian Journal of Educational Technology. – 2011. – Vol. 27, N 7. – P. 1155–1170.

*Baldry A.C., Sorrentino A., Farrington D.P.* Post-Traumatic Stress Symptoms Among Italian Preadolescents Involved in School and Cyber Bullying and Victimization // Journal of Child and Family Studies. – 2019. – N 28. – P. 2358–2364.

*Bauman S.* Cyberbullying in a rural intermediate school: An exploratory study // The Journal of Early Adolescence. – 2009. – Vol. 30, N 6. – P. 803–833.

Bullying in the digital age: A critical review and metaanalysis of cyberbullying research among youth / Kowalski R.M., Giumetti G.W., Schroeder A.N., Lattanner M.R. // Psychological Bulletin. – 2014. – Vol. 140. – P. 1073–1137.

*Cacioppo J.T., Hawkley L.C., Thisted R.A.* Perceived social isolation makes me sad: 5-year cross-lagged analyses of loneliness and depressive symptomatology in the Chicago health, aging, and social relations study // Psychology and Aging. – 2010. – N 25. – P. 453–463.

*Calpbinici P., Arslan F.T.* Virtual behaviors affecting adolescent mental health: The usage of Internet and mobile phone and cyberbullying // Journal of Child and Adolescent Psychiatric Nursing. – 2019. – Vol. 32, N 3. – P. 139–148.

*Chan S.F., La Greca A.M., Peugh J.L.* Cyber victimization, cyber aggression, and adolescent alcohol use: Short-term prospective and reciprocal associations // Journal of Adolescence. – 2019. – Vol. 74. – P. 13–23.

*Cortés A.F. M., De los Ríos O.L. H., Pérez A.S.* Factores de riesgo y factores protectores relacionados con el ciberbullying entre adolescentes: una revisión sistemática risks and protective factors related to cyberbullying among adolescents: a systematic review // Psychologist Papers. – 2019. – Vol. 40, N 2. – P. 109–124.

Cyberbullying and traditional bullying: The experiences od poly-victimization among diverse youth / Myers Z.R., Swearer S.M., Martín M.J., Palacios R. // International Journal of Technoethics. – 2017. – Vol. 8, N 2. – P. 42–60.

Cyberbullying in gifted students: prevalence and psychological well-being in a spanish sample / González-Cabrera J., Tourón J., Machimbarrena J.M., Gutiérrez-Ortega M., Álvarez-Bardón A., Garaigordobil M. // International Journal of Environmental Reserch and Public Health. – 2019. – Vol. 16, N 12. – URL: https://doi.org/10.3390/ijerph16122173 (дата обращения 20.03.2020).

Cyberbullying, problematic internet use, and psychopathologic symptoms among korean youth / Jung Y.E., Leventhal B., Kim Y.S. et al. // Yonsei Medical Journal. – 2014. – Vol. 55, N 3. – P. 826–830.

Cyberbullying, school bullying, and psychological distress: A regional census of high school students / Schneider S., Donnell L., Stueve A., Coulter R. // American Journal of Public Health. – 2012. – Vol. 102. – P. 171–177.

*Del Rey R., Elipe P., Ortega-Ruiz, R.* Bullying and cyberbullying: Overlapping and predictive value of the co-occurrence // Psicothema. – 2012. – Vol. 24, N 4. – P. 608–613.

Do cyberbullies suffer too? cyberbullies' perceptions of the harm they cause to others and to their own mental health / Campbell M.A., Slee P.T., Spears B., Butler D., Kift S. // School Psychology International. – 2013. – Vol. 34, N 6. – P. 613–629.

*Englander E.K.* Cyberbullying and information exposure: User-generated content in post-secondary education // MARC Publications. – 2008. – URL: https://vc.bridgew.edu/marc_pubs/11 (дата обращения 20.03.2020).

Friendship quality and gender differences in association with cyberbullying involvement and psychological well-being / Foody M., McGuire L., Kuldas S., O'Higgins N.J. // Frontiers of Psychology. – 2019. – URL: https://doi.org/10.3389/fpsyg.2019.01723 (дата обращения 20.03.2020).

*Garaigordobil M., Machimbarrena J.M.* Victimization and perpetration of bullying/cyberbullying: connections with emotional and behavioral problems and childhood stress // Psychosocial Intervention. – 2019. – Vol. 28, N 2. – P. 67–73.

*Gordillo I.C., Antelo I.F., Martín-Mora G.* Pueden las víctimas de bullying convertirse en agresores del ciberespacio? Estudio en población adolescente // European Journal of Investigation in Health, Psychology and Education. – 2019. – Vol. 9, N 2. – P. 71–81.

Health-related risks for involvement in bullying among middle and high school youth / Waasdorp T.E., Mehari K.R., Milam A.J., Bradshaw C.P. // Journal of Child and Family Studies. – 2019. – Vol. 28. – P. 2606–2617.

*Herrera-López M., Romera E., Ortega-Ruiz R.* Bullying y cyberbullying en Colombia; coocurrencia en adolescentes rscolarizados // Revista Latinoamericana de Psicología. – 2017. – Vol. 49. – P. 163–172.

*Hinduja S., Patchin J.W.* Cultivating youth resilience to prevent bullying and cyberbullying victimization // Child Abuse and Neglect. – 2017. – Vol. 73. – P. 51–62.

Informe Ejecutivo del Proyecto Ciberastur / González-Cabrera J., Balea-Vazquel A., Vallina-Paco M., Moya A., Laviana-Corte F. // Universidad Internacional de la Rioja (UNIR) y Consejería de Educación y Cultura del Principado de Asturias. – 2017. – URL: https://www.educastur.es/documents/10531/40634/2017–12_con-pub-informes_informe-ciberastur.pdf/a6c9790d-7de4–45a7–9f34-a636b598787f (дата обращения 20.03.2020).

*Kokkinos C.M., Antoniadou N.* Cyber-bullying and cyber-victimization among undergraduate student teachers through the lens of the General Aggression Model // Computers in Human Behavior. – 2019. – Vol. 98. – P. 59–68.

*Kureka A., Josea P.E., Stuartb J.* «I did it for the LULZ»: How the dark personality predicts online disinhibition and aggressive online behavior in adolescence // Computers in Human Behavior. – 2019. – Vol. 98. – P. 31–40.

Latent class analysis of school refusal behavior and its relationship with cyberbullying during adolescence / Delgado B., Martinez-Monteagudo M.C., Ruiz-Esteban C., Rubio E. // Frontiers of Psychology. – 2019. – URL: https://doi.org/10.3389/fpsyg.2019.01916. (дата обращения 20.03.2020).

*Livazovic G., Ham E.* Cyberbullying and emotional distress in adolescents: the importance of family, peers and school // Heliyon. – 2019. – Vol. 5, N 6. – URL: https://doi.org/10.1016/j.heliyon.2019.e01992 (дата обращения 20.03.2020).

*Marcum C.D., Higgins G.E.* Examining the effectiveness of academic scholarship on the fight against cyberbullying and cyberstalking // American Journal of Criminal Justice. – 2019. – Vol. 44. – P. 645–655.

Mechanisms of moral disengagement in the exercise of moral agency / Bandura A., Caprara G.V., Barbaranelli C., Pastorelli C., Regalia C. // Journal of Personality and Social Psychology. – 1996. – Vol. 71, N 2. – P. 364–374.

*Moore P.M., Huebner E.S., Hills K.J.* Electronic bullying and victimization and life satisfaction in middle school students // Social Indicators Research. – 2012. – Vol. 107, N 3. – P. 429–447.

*Nowland R., Talbot R., Qualter P.* Influence of loneliness and rejection sensitivity on threat sensitivity in romantic relationships in young and middle-aged adults // Personality and Individual Differences. – 2018. – Vol. 131. – P. 185–190.

Online hate and harmful content: Cross-national perspectives / Keipi T., Näsi M., Oksanen A., Räsänen P. // London: Taylor & Francis Grou, 2016. – 154 p.

*Peter I.K., Petermann F.* Cyberbullying: A concept analysis of defining attributes and additional influencing factors // Computers in Human Behavior. – 2018. – Vol. 86. – P. 350–366.

*Przybylski A.K., Bowes L.* Cyberbullying and adolescent well-being in England: a population-based cross-sectional study // The Lancet Child & Adolescent Health. – 2017. – Vol. 1, N 1. – P. 19–26.

*Runions K.C., Bak M.* Online moral disengagement, cyberbullying, and cyber aggression // Cyberpsychology, Behavior, and Social Networking. – 2015. – Vol. 18, N 7. – P. 400–405.

*Savage M.W., Tokunaga R.S.* Moving toward a theory: Testing an integrated model of cyberbullying perpetration, aggression, social skills, and internet self-efficacy // Computers in Human Behavior. – 2017. – Vol. 71. – P. 353–361.

School violence and bullying (Education 2030) // Global Status Report. UNESCO. – 2017 – URL: http://unesdoc.unesco.org/images/0024/002469/246970e.pdf (дата обращения 20.03.2020).

Spreading dynamics of a cyber violence model on scale-free networks / Liu W., Li T., Cheng X., Xu H., Liu X. // Physica A. – 2019. – Vol. 531. – URL: https://doi.org/10.1016/j.physa.2019.121752 (дата обращения 20.03.2020).

Student bystander behaviour and cultural issues in cyberbullying: When actions speak louder than words / Ferreira C.P., Simao V.A.M., Ferreira A., Souza S., Francisco S. // Computers in Human Behavior. – 2016. – Vol. 60. – P. 301–311.

*Suler J.* The online disinhibition effect // CyberPsychology and Behavior. – 2004. – Vol. 7, N 3. – P. 321–326.

The «net» of the internet: Risk factors for cyberbullying among secondary-school students in Greece / Athanasiades C., Baldry A.C., Kamariotis T., Kostouli M., Psalti A. // European Journal on Criminal Policy and Research. – 2016. – Vol. 22, N 2. – P. 1–17.

The differential victimization associated with depression and anxiety in cross-cultural perspective: a meta-analysis / Yuchang J., Junyi L., Junxiu A., Jing W., Mingcheng H. // Trauma, Violence & Abuse. – 2019. – Vol. 20, N 4. – P. 560–573.

The impact of cyberbullying and social bullying on optimism, global and school-related happiness and life satisfaction among 10–12-year-old schoolchildren / Navarro R., Ruiz-Oliva R., Larrañaga E., Yubero S. // Applied Research in Quality of Life. – 2013. – Vol. 10. – P. 15–36.

The relationship between bullying victimization and gambling among adolescents / Grande-Gosende A., Richard J., Ivoska W., Derevensky J. // International Gambling Studies. – 2019. – URL: https://doi.org/10.1080/14459795.2019.1652669 (дата обращения 20.03.2020).

*Tudkuea T., Laeheem K., Sittichai R.* Development of a causal relationship model for cyber bullying behaviors among public secondary school students in the three southern border provinces of Thailand // Children and Youth Services Review. – 2019. – Vol. 102. – P. 145–149.

*Wagner A.* E-victimization and e-predation theory as the dominant aggressive communication: the case of cyber bullying // Social Semiotics. – 2019. – Vol. 29, N 3. – P. 303–318.

Which personality traits are related to traditional bullying and cyberbullying? A study with the big five, dark triad and sadism / Geel M.V., Goemans A., Toprak F., Vedder P. // Personality and Individual Differences. – 2017. – Vol. 106. – P. 231–235.

*Wright M.F.* Adolescents' cyber aggression perpetration and cyber victimization: the longitudinal associations with school functioning // Social Psychology of Education. – 2015. – Vol. 18, N 4. – P. 653–666.

*Zych I., Farrington D.P., Ttofi M.M.* Protective factors against bullying and cyberbullying: A systematic review of meta-analyses // Aggression and Violent Behavior. – 2019. – Vol. 45. – P. 4–19.

*Zych I., Ortega-Ruiz R., Marin-Lopez I.* Cyberbullying: A systematic review of research, its prevalence, and assessment issues in Spanish studies // Psicología Educativa. – 2016. – Vol. 22, N 1. – P. 5–18.

# ПРОФЕССИОНАЛЬНЫЙ ВЗГЛЯД

## ЦИФРОВИЗАЦИЯ КАК СОЦИОКУЛЬТУРНАЯ НОВАЦИЯ В РОССИЙСКОМ ОБЩЕСТВЕ

**(Рецензия на монографию Т.Ф. Кузнецовой «Цифровое общество, цифровая культура и гуманитаризация высшего образования: тезаурусный подход»)**


**Костина Анна Владимировна**

Доктор философских наук, доктор культурологии, профессор, проректор по научной работе – директор Института фундаментальных и прикладных исследований Московского гуманитарного университета (Москва, Россия)



***Ключевые слова:*** *цифровая среда; цифровизация; цифровая культура; цифровая экономика.*

**Для цитирования:** Костина А.В. Цифровизация как социокультурная новация в российском обществе. Рецензия на монографию Т.Ф. Кузнецовой «Цифровое общество, цифровая культура и гуманитаризация высшего образования: тезаурусный подход» // Социальные новации и социальные науки. – Москва: ИНИОН РАН, 2020. – № 1. – С. 160–165.

URL: https://sns-journal.ru/ DOI: 10.31249/snsn/2020.01.13

В издательстве Московского гуманитарного университета вышла монография видного российского культуролога профессора Т.Ф. Кузнецовой [Кузнецова, 2020]. Известная своими книгами о философских аспектах гуманитаризации образования [Кузнецова, 1990], истории американской культуры [Кузнецова, 2010], теоретических проблемах культурной картины мира [Кузнецова, 2012], она в последнее время все чаще обращается к культурному ракурсу такого обширного и многообразного процесса как цифровизация [Кузнецова, 2018; Кузнецова, 2019 a; Кузнецова, 2019 b]. Этот процесс уже несколько десятилетий идет в мире и активно развивается в России.

На уровне Правительства РФ с 2017 г. уделяется первостепенное внимание созданию цифровой экономики – принятие распоряжением председателя Правительства РФ № 1632-р федеральной программы «Цифровая экономика Российской Федерации» об этом наглядно свидетельствует. Однако, как показывает Т.Ф. Кузнецова в своей книге, стремление выйти на один уровень с мировыми лидерами цифровизации, важное для развития страны, оказалось оторванным от социокультурных процессов, протекающих в России. Это делает принятые планы выполнимыми только частично – за счет средств управления и применения новых технологий, но без населения. Автор книги показывает, что цифровизация не может быть сведена лишь к экономическим достижениям, это гораздо более широкий социальный процесс. «Цифровизация в этом смысле затрагивает не только экономику, сферу производства и потребления новых предметов по материалам, из которых они сделаны, по их функции, включение в повседневность. Она становится основой культуры и на наших глазах меняет как саму эту культуру, так и общество, которое нас окружает. А значит – и нас самих» [Кузнецова, 2020, с. 8].

Т.Ф. Кузнецова не стремится показать цифровую экономику в алармистских тонах, увидеть в ней символ бездуховности и ухода человека в мир, лишенный культурных ценностей. Напротив, цифровая экономика связывается ею со стратегией развития России в XXI в. То, что в федеральной программе «Цифровая экономика Российской Федерации» отсутствует раздел по культуре, вовсе не свидетельствует, по Т.Ф. Кузнецовой, об утере этого аспекта из российского варианта новой экономической политики: у программы другие цели, она не представляет цифровизацию в глобальном масштабе. Приписывать ей всеохватность было бы поверхностным подходом, хотя такой взгляд часто встречается в литературных источниках, особенно у культурологов.

Т.Ф. Кузнецова разделяет позицию А.А. Аузана – одного из ведущих отечественных экономистов, декана экономического факультета МГУ им. М.В. Ломоносова [Аузан, 2013]. В его концепции цифровой экономики на первое место выдвигается проблема культуры: «Экономическая эффективность становится, таким образом, фактом культурной предрасположенности к ее актив-

ным трансформациям в той или иной стране, регионе и т.д.» [Кузнецова, 2020, с. 16]. Это принципиально значимо и для теории, и для практики в экономической сфере.

Но Т.Ф. Кузнецова идет дальше, видя за фасадом цифровой экономики перемены в мире и России, которые связываются со становлением цифрового общества и цифровой культуры. Нельзя сказать, что эти словосочетания используются впервые. Напротив, в новой институциональной экономике, которая выступает в качестве теоретического основания цифровой экономики, «человеческий фактор» и культурные аспекты очень заметны. Однако, как показывает в книге Т.Ф. Кузнецова, в данном подходе есть и сильные, и слабые стороны. Понятно, в чем сила. В чем же слабость? Она видится автору в том, что «школа новой институциональной экономики исходит преимущественно из западной системы ценностей. Культура тоже предстает здесь в конечном счете (даже, когда говорится о неевропейских странах) в европоцентристской модели, с ориентацией на ее единство и глобальное значение для мира» [Кузнецова, 2020, с. 19].

Вместе с тем культура в целом и цифровая культура в частности могут трактоваться поразному. Поэтому за уже привычными словосочетаниями часто скрываются совсем несхожие представления. Как пишет Т.Ф. Кузнецова, «в понимании цифровой культуры наметились две линии, которые не пересекаются. Одна трактует культуру через артефакты. Другая усматривает в ней монстра, порождаемого всеобщей цифровизацией, культура здесь скорее название, чем основание для исследования» [Кузнецова, 2020, с. 24].

Взгляд автора на культуру учитывает сложившуюся ситуацию. Но все же в его основе лежат представления об ансамбле ценностей, передаваемых от поколения к поколению и обеспечивающих устойчивость общества, цифрового в том числе. Вот почему в книге появляется тезаурусный подход, редко используемый на фоне общественного внимания к изменениям, порожденным цифровизацией. Тезаурусный анализ вынесен в подзаголовок работы, и, по сути, представляет основу культурологического ракурса темы, в которой рассматриваются планы, проблемы и вызовы цифровой экономики для России.

Автор показывает, что тезаурусный подход к цифровой культуре наиболее адекватен при социокультурном (а не лингвистическом) понимании тезауруса. «Тезаурус представляет собой определенную *конструкцию знаний* у каждого человека, группы людей, социальных общностей и т.д. У этой конструкции два основных назначения. Первое – *ориентация* в окружающей среде. Вторая – *саморазвитие*, создание нового (сверхориентация). И в том и в другом случае субъекту (человеку, группе и т.д.) нужны не все знания, какие существуют в мире, а те, которые дают возможность для решения ориентационных и сверхориентационных задач. Такая конструкция знаний отличается от конструкции науки. Если в науке основа систематизации знаний строится по модели от общего к частному и единичному, то в тезаурусе – от *своего* к *чужому*. В таком случае для того, чтобы что-

то вошло в тезаурус, оно должно быть *освоено*, т.е. стать *своим*. Эта смена ракурса одновременно означает то, что тезаурусы выступают как *субъектно организованное гуманитарное знание*» [Кузнецова, 2020, с. 111]. Понимание тезауруса Т.Ф. Кузнецовой соответствует его толкованию, которое дали В.А. и Вл.А. Луковы, подчеркивающие, что «тезаурус – это полный систематизированный свод освоенных социальным субъектом знаний, существенных для него как средство ориентации в окружающей среде, а сверх этого также знаний, которые непосредственно не связаны с ориентационной функцией, но расширяют понимание субъектом себя и мира, дают импульсы для радостной, интересной, многообразной жизни» [Луков, Луков, 2013, с. 3].

Для выявления характерных черт цифровой культуры важно понять, что тезаурус как накопленные знания заведомо неполон и в то же самое время вполне достаточен для достижения определенных целей. Цифровая культура, представленная как совокупность тезаурусов, не описывается в категориях формальной логики и не может быть сведена к научному знанию, хотя это вроде бы соотносится с ее названием. В центре тезауруса стоит культурная картина мира, т.е. «определенное понимание человеком окружающей его действительности. Это понимание строится на системе ценностей, освоенных данным субъектом. Потому в структуре тезауруса его строительным материалом являются в первую очередь *концепты* – некоторые ментальные и эмоционально окрашенные сращения понятия и образа» [Кузнецова, 2020, с. 112].

Исходя из этой теоретической конструкции культурной картины мира, автор рассматривает становления цифрового общества в России. Данный подход позволяет Т.Ф. Кузнецовой сделать следующий вывод: «…цифра еще не вошла в тезаурусы и тем более в культурную картину мира значительной части россиян. В этом смысле пока нельзя говорить о том, что в России уже сложилось цифровое общество и присущая ему цифровая культура. Это, конечно, не значит, что цифровая инфраструктура как комплекс технологий и продуктов, на них построенных и обеспечивающих жизнедеятельность людей… не присутствует в стране» [Кузнецова, 2020, с. 116]. Автор убедительно доказывает, что использование новых технологий не решает содержательно вопрос культуры, которая складывается на протяжении веков в разных социокультурных обстоятельствах и касается жизни миллионов людей. Противоречий между современными техническими возможностями и готовностью людей строить на этой основе новый тип общества накопилось немало. И их уже невозможно не замечать, особенно при реализации крупных и перспективных социальных проектов.

В связи с этим Т.Ф. Кузнецова пишет: «По нашему мнению, выход из культурного тупика все же есть. Он решает не все задачи, но обладает той характеристикой “критической массы”, которую единственно и можно применить, решая эту актуальную для России и всего мира проблему. Итак, такую характеристику можно применить к системе образования, и состоять она будет в гу-

манитаризации высшего образования» [Кузнецова, 2020, с. 126]. Не случайно третья глава книги посвящена гуманитаризации высшего образования в цифровом обществе – это развитие авторской идеи по преодолению культурного аспекта разрыва между цифровой экономикой и цифровым обществом.

Т.Ф. Кузнецова уже неоднократно обращалась к данной теме, выделяя ее философский аспект, а также новые возможности и пути преподавания философских дисциплин в вузах. По всем этим направлениям велись активные дискуссии среди отечественных философов в 1980-х годах. Но времена изменились, и тема теперь звучит совсем иначе, чем в прошедшие годы. Точнее, изменился контекст многих бывших актуальными вопросов – и это видно в рассматриваемой работе. По-прежнему злободневным остается, например, сочетание жанров философствования, соединение трактатов и публицистики, эссе и художественных образов литературы. Но все-таки центр дискурса сместился. Сейчас центральное звено высшего образования «не передача знаний, а формирование понимания происходящего. С учетом того, что представляет собой современное общество, и того, каким оно становится в перспективе, формирование понимания того, что происходит и прорывается в действительность, выражает тот новый аспект гуманитаризации высшего образования, который оказался столь необходимым, чтобы общество развивать, а не порождать абсурд происходящего» [Кузнецова, 2020, с. 160].

Современная гуманитаризация высшего образования в России поменяла свое назначение по сравнению с тем, какой она представлялась несколько десятилетий назад, когда о цифровизации у нас не слышали, а на Западе это была некая утопия будущего счастливого общества. Она (гуманитаризация) теперь «выступает как контрфорс[1], с одной стороны, большой разницы российских регионов для усвоения цифрового общества и цифровой культуры, а, с другой, возможности цифровой культуры превратиться в цифровую контркультуру» [Кузнецова, 2020, с. 169].

Монография «Цифровое общество, цифровая культура и гуманитаризация высшего образования: тезаурусный подход» ставит вопрос о цифровой культуре в момент ее зарождения в России. Сейчас многие черты еще не определились и не осознаются как будущее нашего общества. Что-то изменится, и предположить характер таких изменений трудно, а то и невозможно. Но именно в таких условиях – условиях зарождения новых культурных тенденций – важно их заметить и начать осмысливать, опираясь на многовековую традицию развития мировой и отечественной культуры. В этом видится значение появления новой книги Т.Ф. Кузнецовой.

## Список литературы

*Аузан А.А.* Экономика всего. Как институты определяют нашу жизнь. – М.: Манн, Иванов и Фербер, 2013. – 160 с.
*Кузнецова Т.Ф.* Философия и проблема гуманитаризации образования / Филос. об-во СССР. – М., 1990. – 117 с.

[1] В данном контексте – противодействующая сила. – *Прим. ред.*

*Кузнецова Т.Ф.* Культурная картина мира: теоретические проблемы. – М.: ГИТР, 2012. – 250 с.
*Кузнецова Т.Ф.* Цифровое общество в свете культурологии // Горизонты гуманитарного знания. – 2018. – № 1. – С. 27–36.
*Кузнецова Т.Ф.* Цифровизация и цифровая культура // Горизонты гуманитарного знания. – 2019 a. – № 2. – С. 96–102.
*Кузнецова Т.Ф.* Цифровизация как культурная ценность и цифровые технологии // Горизонты гуманитарного знания. – 2019 b – № 5. – С. 3–13.
*Кузнецова Т.Ф.* Цифровое общество, цифровая культура и гуманитаризация высшего образования: тезаурусный подход. – М.: Изд-во Моск. гуманит. ун-та, 2020. – 192 с.
*Кузнецова Т.Ф., Уткин А.И.* История американской культуры. – М.: Человек, 2010. – 432 с.
*Луков В.А., Луков Вл.А.* Тезаурусы II: Тезаурусный подход к пониманию человека и его мира. – М.: Изд-во Нац. ин-та бизнеса, 2013. – 640 с.

# СОЦИАЛЬНЫЕ НОВАЦИИ
# И
# СОЦИАЛЬНЫЕ НАУКИ

**Научный журнал**

**№ 1 (1) / 2020**

## ЦИФРОВИЗАЦИЯ И БЕЗОПАСНОСТЬ:
## ЛИЧНОСТЬ, БИЗНЕС, ГОСУДАРСТВО

Техническое редактирование
и компьютерная верстка В.Б. Сумерова
Корректор М.П. Крыжановская

Институт научной информации по общественным наукам РАН
117997 Москва, Нахимовский пр., д. 51/21 e-mail: inion@bk.ru

Подписано на выход в свет – 3/VI – 2020 г.

Формат 60×90/8 Уч.-изд.л. 11,3