



2020

Цифровые технологии и кибербезопасность в контексте распространения COVID-19

Дайджест подготовлен
Департаментом международного и
регионального сотрудничества СП РФ

Оглавление

I. Влияние COVID-19 на процессы цифровизации.....	2
1. Тренды.....	2
1.1. Ускорение перехода к цифровой экономике	2
1.2. Проблема цифрового разрыва.....	5
2. Цифровые технологии в борьбе с COVID-19	7
2.1. Сбор данных о физиологическом состоянии граждан в связи с распространением вируса и вопросы защиты персональных данных	8
2.2. Открытые данные и источники данных о COVID-19.....	13
2.3. Робототехника и технологии	16
2.4. Суперкомпьютеры и поиск методов лечения	19
2.5. Новые технологические стартапы	22
3. Дистанционная работа и образование	23
3.1. Адаптация к цифровому формату трудовой деятельности	24
3.2. Онлайн-обучение: перспективы и вызовы.....	25
II. Риски и угрозы цифровому развитию.....	28
1. Факторы, влияющие на кибербезопасность	29
2. Глобальные угрозы	30
2.1. Кибератаки: вредоносные домены, вредоносные программы и勒索ware в сети.....	30
2.2. Мошенничество и контрафактная торговля средствами индивидуальной защиты и противовирусными лекарственными средствами.....	32
2.3. Информационные угрозы в эпоху COVID-19	33
3. Принимаемые меры	35
3.1. Взаимодействие на государственном уровне	35
3.2. Взаимодействие с частными партнерами.....	35
3.3. Помощь пострадавшим сторонам.....	36
3.4. Взаимодействие с гражданами	36
3.5. Меры профилактики.....	36
III. Выводы и рекомендации.....	38

I. Влияние COVID-19 на процессы цифровизации

1. Тренды

1.1. Ускорение перехода к цифровой экономике

Распространение COVID-19 способствует изменению экономической и социальной жизни во многих странах. Одним из ярких последствий текущей пандемии уже сейчас можно назвать ускоренное внедрение цифровых технологий в самых разных областях.

В рамках вводимых правительствами ограничений на передвижение и мер социального дистанцирования бизнес и потребители активно осваивают цифровые решения для продолжения деятельности в удаленном формате. Цифровизация способствует переходу в онлайн-среду медицины, трудовой деятельности, образования, позволяет совершать онлайн-покупки, получать больше данных о распространении вируса и обмениваться информацией об исследованиях. Развитие указанного тренда говорит не только о назревшей потребности, но и о созданной материальной базе для широкого использования цифровых технологий.

По сравнению с ситуацией мирового финансового кризиса 2008 г., за прошедшие 12 лет количество пользователей сети Интернет выросло с 1,6 до 4,1 млрд, а количество используемых в мире смартфонов достигло 3,2 млрд. Удельный вес интернет-пользователей среди мирового населения за то же время вырос с 23% до 54%, количество людей, пользующихся сервисами интернет-покупок, удвоилось, а объем розничной торговли в сети Интернет вырос с 1 до 3,8 трлн долл. США.

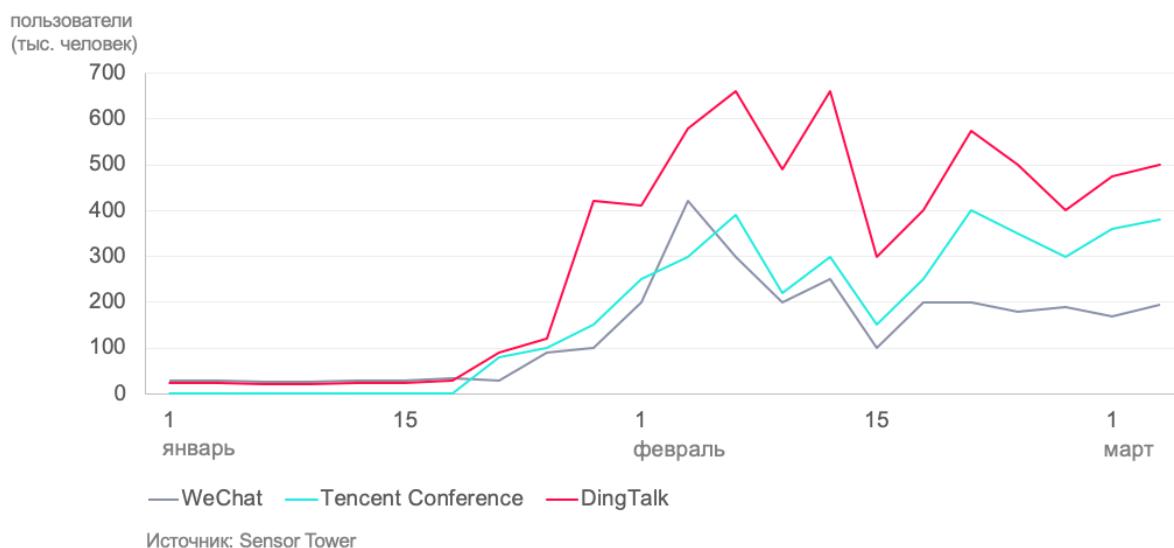
Из шести основных трендов цифровизации, которые ЮНКТАД отмечает в контексте кризиса [COVID-19](#), три непосредственно связаны с повсеместным ускорением перехода к цифровой экономике:

- **Удаленная работа и использование технологий связи**

В связи с распространением COVID-19 в мире **все больше людей работает удаленно, используя сервисы для видеоконференций и мессенджеры**. Увеличился спрос на использование таких программ, как Microsoft Teams, Skype, Cisco's Webex и Zoom.

В Китае использование сервисов для удаленной работы от WeChat, Tencent и Ding значительно выросло в конце января 2020 г., когда вступили в силу ограничения, связанные с COVID-19.

Скачивание приложений для удаленной работы в Китае



Использование онлайн-платформ стимулирует развитие **облачных технологий** для хранения и анализа данных, повышает спрос на аренду таких сервисов от технологических компаний (Amazon Web Services, Microsoft, Tencent и Alibaba).

Кризис также способствовал переходу школ и университетов на дистанционный формат обучения. **Цифровые инструменты и онлайн-тренинги** позволяют учителям и преподавателям оставаться на связи с учащимися.

- **Негативное воздействие на некоторые цифровые платформы**

Кризис, вызванный распространением COVID-19, **оказал негативное воздействие** на цифровые платформы преимущественно в сфере передвижения и путешествий. К этой группе можно отнести сервисы, связанные с перевозками (Uber, Lyft, Didi Chuxing), а также сервисы по аренде жилья (Airbnb, Booking.com). Данный тренд отражает общий спад в отраслях путешествий и туризма во время пандемии.

- Изменение потребительских привычек

В то же время распространение COVID-19 привело к **увеличению объемов электронных продаж**. Например, в США наблюдается рост онлайн-продаж в сфере доставки еды, кормов для домашних животных. Значительный рост коснулся некоторых позиций медицинских товаров. По данным компании RecVue, [наблюдаются всплеск запросов, связанных с покупкой антисептиков для рук и антибактериального мыла](#).

Крупнейший в мире онлайн-ретейлер Amazon принял решение о найме дополнительных 75 тыс. сотрудников в связи с увеличением количества заказов во время пандемии COVID-19. Учрежден специальный фонд размером в 25 млн долл. США, «предназначенный для облегчения положения партнеров, в частности водителей грузовиков и сезонных внештатных работников»¹.

Китайский онлайн-ретейлер JD.com сообщил об увеличении объемов продаж продовольственных товаров на 215% до 15 тыс. тонн за период в десять дней в конце января – начале февраля 2020 г. (по сравнению с аналогичным периодом прошлого года)².

Агентство ЕС по вопросам кибербезопасности (англ. – *European Union Agency for Cybersecurity*) [полагает](#), что рост электронных продаж способствует **ускорению цифровой трансформации предприятий, особенно среднего и малого бизнеса**, вынужденного расширять свое онлайн-присутствие для того, чтобы выжить в текущих условиях. Предприятия среднего и малого бизнеса составляют 99% от числа всех компаний в Европе. Хотя 77% таких предприятий имеют собственные веб-сайты, только 17% продают товары через Интернет. В то же время около 41% европейцев обеспокоено безопасностью онлайн-платежей³.

Другую область, где наблюдается увеличение активности пользователей, представляют **стриминговые сервисы**. Закрытие театров и кинотеатров привлекло новую аудиторию для стриминговых сервисов и видео-хостингов Netflix, HBO, Youtube и др. Закрытие школ также способствует увеличению спроса в данной области, поскольку дети и подростки проводят больше времени дома.

¹ Amazon объявила о найме 75 тыс. работников дополнительно из-за роста заказов / Сайт ТАСС / <https://tass.ru/ekonomika/8233107>

² The COVID-19 Crisis: Accentuating the Need to Bridge Digital Divides / Сайт ЮНКТАД / https://unctad.org/en/PublicationsLibrary/dtlinf2020d1_en.pdf

³ Tips for cybersecurity when buying and selling online / Сайт Агентства ЕС по вопросам информационной безопасности / <https://www.enisa.europa.eu/news/enisa-news/tips-for-cybersecurity-when-buying-and-selling-online>

Большинство цифровых решений предлагаются и поддерживаются достаточно небольшим числом крупнейших платформ, созданных в США или Китае. Например, в отчете ЮНКТАД [«Цифровая экономика – 2019»](#) отмечается, что на долю компании Google приходится 90% всего рынка поисковых запросов в Интернете, на долю Facebook – две трети рынка социальных сетей, на долю Amazon – 40% от общемирового рынка ритейла. Ускорение темпов цифровизации способствует укреплению их позиций на рынках. **Эффект сетевой выгоды**, а также их способность отслеживать, извлекать и анализировать информацию, позволили получить таким компаниям преимущество. Впоследствии полученные данные могут быть трансформированы в цифровые знания и монетизированы различными способами.

Изменения в поведении общества, произошедшие во время распространения COVID-19, будут иметь долгосрочные последствия. **Многие организации и пользователи будут более активно использовать цифровые решения**, так как во время кризиса выработают к этому определенную привычку.



1.2. Проблема цифрового разрыва

Использование данных и цифровых платформ предоставляет странам дополнительные возможности для преодоления вызовов развития. В то же время, несмотря на быстрое освоение технологий, **сохраняются значительные цифровые разрывы – существенные**

различия в скорости внедрения и освоения цифровых технологий. Кризис, вызванный COVID-19, продемонстрировал существующее расслоение как между странами, так и внутри них.

Как показывают [публикации](#), подготовленные ЮНКТАД, у наименее развитых стран существуют значительные ограничения в различных сферах, связанных с цифровыми технологиями, – от инфраструктуры информационно-коммуникационных технологий и сервисов в области платежей до квалификации работников и формирования нормативно-правовой базы. Реагируя на эти трудности, они пытаются использовать доступные цифровые возможности для преодоления кризиса, вызванного распространением COVID-19.

В Сенегале Министерство торговли, малого и среднего бизнеса планирует создать платформу для объединения предприятий с цифровым потенциалом с целью осуществления доставки товаров первой необходимости⁴.

Цифровой разрыв между государствами особенно наглядно наблюдается в сфере образования, где возможности учащихся пользоваться услугами онлайн-обучения могут существенно различаться в зависимости от наличия домашнего компьютера и доступа к сети Интернет, уровня доходов семьи и степени подготовленности школ.

По данным Международной программы по оценке образовательных достижений учащихся ОЭСР (англ. – *Programme for International Student Assessment*)⁵, в таких странах, как Дания, Словения, Норвегия, Польша, Литва, Исландия, Австрия, Швейцария и Нидерланды 95% учащихся могут воспользоваться домашним компьютером, в то время как для Индонезии этот показатель составляет только 34%.

Среди государств с низким уровнем дохода более 75% не предлагают никаких форм дистанционного обучения. Но даже когда правительства таких стран принимают меры по организации образования в режиме онлайн, они не охватывают большинство учащихся, поскольку только 36% жителей этих стран имеют доступ в Интернет⁶.

⁴ The COVID-19 Crisis: Accentuating the Need to Bridge Digital Divides / Сайт ЮНКТАД / https://unctad.org/en/PublicationsLibrary/dtlinf2020d1_en.pdf

⁵ В рамках программы были получены данные о 600 тыс. учащихся в возрасте 15 лет за 2018 г.

⁶ <https://www.brookings.edu/research/school-closures-government-responses-and-learning-inequality-around-the-world-during-covid-19/>

Цифровой разрыв также существует и внутри стран: в США каждый ученик из экономически благополучной школы обладает доступом к домашнему компьютеру, но только 3 из 4 учеников из неблагополучных школ имеют такую возможность. В Перу эти показатели составляют 88% и 17% соответственно. В Мексике 94% учащихся из благополучных семей обладают доступом к сети Интернет, тогда как в неблагополучных семьях этот показатель составляет 29%⁷.

Очевидно, что условия изоляции усугубили эти проблемы. Для 18 млн американских домохозяйств, вообще не имеющих доступа в Интернет, за последние несколько недель «цифровой разрыв» стал лишь более болезненным и очевидным, будь то школьники, которые не могут участвовать в онлайн-занятиях, либо взрослые, которые не могут работать удаленно, либо просто семья, которая не может заказать доставку продуктов на дом.

Учитывая возрастающую роль качественного доступа в Интернет по мере продолжения цифровизации общества и экономики, пандемия COVID-19, без сомнения, подтолкнет правительства к принятию новых мер по ликвидации «цифрового разрыва» в форме государственных инвестиций в инфраструктуру или более жесткого регулирования (по аналогии с сектором электроэнергетики), а также вызовет очередной всплеск программ по увеличению количества подключений и распространению устройств для доступа в Интернет⁸.

Один из недавних законопроектов Конгресса США о помощи в восстановлении от последствий пандемии COVID-19 предусматривает кредиты на сумму 125 млн долл. США телекоммуникационным компаниям для создания инфраструктуры доступа в интернет в сельской местности⁹.

2. Цифровые технологии в борьбе с COVID-19

⁷ Learning remotely when schools close: How well are students and schools prepared? Insights from PISA / Сайт ОЭСР / https://read.oecd-ilibrary.org/view/?ref=127_127063-iiwm328658&title=Learning-remotely-when-schools-close

⁸ How COVID-19 will change the nation's long-term economic trends, according to Brookings Metro scholars / <https://www.brookings.edu/research/how-covid-19-will-change-the-nations-long-term-economic-trends-brookings-metro/>

⁹ <https://www.brookings.edu/blog/techtank/2020/04/02/why-the-internet-didnt-break/>

2.1. Сбор данных о физиологическом состоянии граждан в связи с распространением вируса и вопросы защиты персональных данных

Одним из наиболее заметных последствий кризиса в связи с COVID-19 стало массовое применение технологических решений для сбора информации о распространении вируса и физиологическом состоянии граждан. Это стало возможным ввиду удешевления и, соответственно, широкого использования гражданами смартфонов и переносных устройств (англ. – *wearables*), которые собирают данные об образе жизни их владельцев. Возникает вопрос, каким образом можно использовать их эффективнеедля ускорения поиска лечения COVID-19 или, например, деменции, или рака.

Во время кризиса, вызванного распространением COVID-19, наблюдается скачок в применении технологий по **отслеживанию социальных контактов**.

В целях привлечения как можно большего количества пользователей к программе отслеживания и предотвращения распространения коронавирусной инфекции, мировые технологические лидеры Apple и Google достигли беспрецедентных договоренностей по ликвидации технических препятствий для обмена данными между платформами iOS и Android. В ближайшее время будут запущены совместимые инструменты для разработчиков, позволяющие сделать официальные приложения учреждений здравоохранения доступными для пользователей обеих платформ, а в среднесрочной перспективе производители планируют встроить в свои аппараты общую технологию отслеживания близких контактов по протоколу Bluetooth. В компаниях подчеркивают, что конфиденциальность, прозрачность и добровольность являются главными приоритетами при разработке¹⁰.

Исследовательским институтом в г. Сан-Диего (Калифорния) была представлена работа «Обнаружение» (англ. – DETECT – Digital Engagement & Tracking for Early Control & Treatment). В работе анализируются данные о сердечной деятельности, а также информация о состоянии организма во время бодрствования и сна. Все данные были получены через переносные устройства – браслеты FitBit, умные часы Apple и Garmin, кольца Oura.

Группа ученых Оксфордского университета провела математическое моделирование темпов распространения коронавирусной инфекции в двух различных случаях: когда

¹⁰ Apple и Google создают технологию отслеживания контактов для борьбы с COVID-19 / Сайт Apple / <https://www.apple.com/ru/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/>

для сдерживания распространения изолируются только те, кто демонстрирует симптомы заболевания, и когда на карантин помещаются также все те, кто находился с ними в непосредственном контакте. Основной вывод: скорость распространения COVID-19 настолько высока, что изолирование лишь граждан с симптомами заболевания, а также выявление их контактов и, соответственно, других возможных заражений в «ручном режиме», недостаточно для эффективного сдерживания. В то же время утверждается, что успех гарантирован, если отслеживание контактов будет осуществляться быстрее, эффективнее и в большем масштабе, например, с помощью мобильных приложений. При этом авторы исследования заявляют, что приложения, собирающие информацию и немедленно уведомляющие пользователя в случае подтверждения диагноза у кого-либо из его близких контактов, будут полезным лишь при массовом использовании. Кроме того, по мнению авторов, в таком случае для сдерживания эпидемии будет достаточно применения ограничительных мер лишь к потенциально зараженным гражданам без необходимости массовых карантинных мероприятий, губительных для общества¹¹.

Специалисты Школы общественного здравоохранения Университета Джонса Хопкинса провели [обзор](#) основных технологических решений, применявшихся в разных странах для отслеживания контактов.

Успех мобильных приложений, использованных в КНР, объясняется глубокой интеграцией с базами данных Министерства транспорта, железных дорог, управления гражданской авиации и государственной комиссии по здравоохранению, а также использованием ранее созданной инфраструктуры для отслеживания перемещений граждан.

В Сингапуре отслеживание потенциальных контактов проводится на основе анализа близости устройств по данным протокола беспроводной связи Bluetooth без учета личности пользователя и перемещений. Данные отправляются органам власти не на постоянной основе, а лишь в случае подтверждения диагноза у какого-либо пользователя и с его согласия, а не востребованные в течение 21 дня данные автоматически удаляются.

При этом возникает целый комплекс вопросов, связанный с приватностью и защитой личных данных. В силу культурно-исторических особенностей различных стран могут существенно отличаться степень «опеки» со стороны государственных органов,

¹¹ Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing / <https://science.sciencemag.org/content/early/2020/04/09/science.abb6936>

которую готовы принять граждане, конкретные формы внедрения технологических решений и гарантии защиты данных и неиспользования их в отличных от заявленных целях.

Например, как [отмечается](#) в том же обзоре Университета Джонса Хопкинса, в США многие технологические решения, нашедшие применение в других странах, могут столкнуться с неприятием со стороны общества ввиду традиционно чувствительного отношения к неприкосновенности частной жизни. Чтобы граждане были уверены в сохранности конфиденциальной информации и не подорвали массовое использование таких технологий для отслеживания контактов, что лишит их какого-либо смысла и эффективности, потребуется грамотное информационное сопровождение со стороны правительства.

В этом плане из американских приложений выделяется [разработка Массачусетского технологического института](#), которая позволяет объединить как **обезличенные пользовательские данные** о последних местонахождениях, так и **результаты опросов пациентов медицинскими работниками**. Это позволяет рассылать уведомления гражданам, которые пересекались приблизительно в одном месте и в одно время с зараженными лицами.

Тем не менее, несмотря на заверения разработчиков различных решений, **общественность** разных стран **не может не задаваться вопросами об уместности и целесообразности** применения конкретных технологий сбора и передачи данных.

Есть немало примеров применения технологий для борьбы с COVID-19, выглядящего достаточно обоснованным. Один из них – [совместная разработка Медицинского подразделения компании General Electric \(GE Healthcare\) и Microsoft](#), основанная на применении облачной технологии, которая позволяет больницам **в режиме реального времени** **визуализировать показания аппаратов ИВЛ** и своевременно **выявлять пациентов, наиболее подверженных риску** ухудшения состояния. Еще один пример – облачный сервис Microsoft Azure и технологии искусственного интеллекта применяются в проекте Microsoft Healthcare Bot service, позволяющем службам неотложной медицинской помощи легко создавать собственных чат-ботов для проверки людей на потенциальные симптомы. Такой виртуальный помощник обрабатывает несравненно больше запросов, чем колл-центр, освобождая человеческие ресурсы для оказания непосредственной неотложной помощи пациентам. С марта

2020 г. организациями здравоохранения создано 1230 таких ботов для оценки симптомов коронавирусной инфекции, которыми воспользовались 18 млн человек¹².

Несколько более спорным видится пример применения цифровых технологий, предусмотренный [Всеобъемлющим планом по выявлению зараженных коронавирусом и отслеживанию их контактов](#), разработанным Университетом Джонса Хопкинса в помощь правительству США и организациям здравоохранения. Речь идет об использовании технологий «интернета вещей» и умных термометров, интегрированных с системами мониторинга симптомов на общенациональном уровне, предоставляющих дополнительный источник данных для анализа распространения инфекции. Подобная база данных и карта показаний была создана американским производителем умных термометров, компанией Kinsa Health, что [позволило отследить](#) эффективность мер по изоляции населения на динамику симптомов.

В некоторых случаях вопрос использования персональных данных встает более остро.

Польские специалисты разработали приложение «Домашний карантин», которое несколько раз в день случайным образом присыпает требование загрузить фотографию владельца телефона (сэлфи) в течение 20 минут. Если пользователь проигнорировал оповещение, то к нему может приехать полиция¹³.

После появления подобных трендов и критики со стороны активистов Европейское управление по защите данных (англ. – European Data Protection Supervisor) предложило создать **единое общеевропейское приложение** для смартфонов. [Планируется](#), что приложение будет использоваться для отслеживания распространения коронавируса и будет отвечать требованиям о защите персональных данных ЕС. На стадии разработки находится Общеевропейская платформа отслеживания контактов с сохранением анонимности (Pan European Privacy-Preserving Proximity Tracing, PEPP-PT), основанная на технологии Bluetooth¹⁴.

¹² <https://news.microsoft.com/transform/how-international-health-care-organizations-are-using-bots-to-help-fight-covid-19/>

¹³ Коронавирус под наблюдением: как чиновники устанавливают цифровой контроль за гражданами / Сайт журнала НОЖ / <https://knife.media/digital-control/>

¹⁴ Bloomberg School of Public Health Research, Johns Hopkins University. Review of Mobile Application Technology to Enhance Contact Tracing Capacity for COVID-19 / <https://www.centerforhealthsecurity.org/resources/COVID-19/COVID-19-fact-sheets/200408-contact-tracing-factsheet.pdf>

В статье, опубликованной на сайте Всемирного экономического форума (ВЭФ), [«Как восстановить конфиденциальность данных после пандемии коронавируса»](#) указывается, что при обычных обстоятельствах медицинские данные о пациентах должны храниться в тайне. Предоставление данных частным компаниям, даже в интересах общественного здравоохранения, вызывает обеспокоенность, поскольку эти данные представляют существенную коммерческую ценность. Например, они могут оказаться ценными для рекламных агентств, которые сотрудничают с фармацевтическими и медицинскими компаниями. Они также могут быть использованы страховыми компаниями для отслеживания истории болезни при принятии решений. Базы данных, содержащие сведения о личностях с привязкой к мобильному телефону, также представляют ценность, особенно для рынка потребительских товаров.

В материалах ВЭФ содержится [сценарий](#), при котором для этих целей разрабатываются **специальные сертифицированные приложения**, в автоматическом режиме передающие данные со смартфонов и переносных устройств. Эти данные **зашифровываются, благодаря чему становятся анонимными**, и только та часть информации, которая имеет отношение к исследуемому вопросу, может быть использована (подобно тому, как сейчас в Интернете покупается и продается музыка).

Предполагается, что применение **технологии блокчейн** может гарантировать, что данные не используются для других целей. Возможен сценарий, при котором пользователи будут предоставлять анонимные данные для ускорения поиска лечебных препаратов, а затем предоставлять часть данных бесплатно бизнесу. Обрабатывая данные со всего мира, алгоритмы машинного обучения будут выявлять **тренды, которые не смогли обнаружить люди**, и предлагать рекомендации.

Ценность таких данных может определяться на специальной бирже, а сама информация может быть зашифрована с помощью токена (*англ. – tokenized*) для сохранения анонимности владельца. **Появление бирж данных** – это реальность, которая может наступить в скором времени.

Очевидно, что **проблема защиты персональных данных, их использования исключительно в заявленных целях – один из наиболее острых вопросов в ситуации с кризисом COVID-19**. Можно прогнозировать, что **его решение станет новой формой общественного договора между государствами и их гражданами**, при этом изменения,

по всей видимости, произойдут практически во всех странах мира. Значительно изменится рынок товаров и услуг, предлагающих решения как по сбору данных, так и по их защите.

Информацию о применении цифровых технологий в сфере здравоохранения можно также найти в [дайджесте](#) «Эпидемия коронавируса: реагирование национальных систем здравоохранения».

2.2. Открытые данные и источники данных о COVID-19

Обеспечение общества открытой и доступной информацией становится ключевой ценностью в периоды глобальных кризисов.

Иван Бегтин, заместитель директора Центра экспертно-аналитических и информационных технологий Счетной палаты Российской Федерации, определяет **открытые государственные данные** как публичную государственную информацию, предоставляемую публике в цифровом виде посредством сети Интернет в форме, допускающей последующий анализ и повторное использование¹⁵. Сегодня открытые данные переходят из категории государственной информации в общемировой формат.

Главная цель раскрытия государственных данных – побудить граждан к их повторному использованию, дать им инструмент создавать и развивать общественное благо, чтобы коммерческий сектор мог предлагать инновационные продукты на конкурентной основе. Это нужно для того, чтобы формировать среду деятельной гражданской критики. Любой человек, обладающий техническими навыками, мог бы создать своими руками общественно полезный сервис¹⁶.

Статистические ведомства государств и международных организаций, в частности, Евросоюза, уже несколько лет не просто публикуют статистические отчеты и бюллетени, но и размещают на собственных сайтах всю накопленную ими статистику в форме, пригодной для повторного использования, – специальных форматах для, так называемой, машинной обработки.

¹⁵ <https://m.polit.ru/article/2010/06/03/opendata/>

¹⁶ <https://m.polit.ru/article/2010/06/03/opendata/>

В период пандемии источники информации и данных о распространении нового коронавируса COVID-19 стали весьма ценным ресурсом, который используют в своей деятельности не только граждане, но и СМИ, НКО, государственные структуры. Данные собираются как официальными исследовательскими сообществами и статистическими службами, так и неформальными группами активистов.

К данным предъявляются следующие **требования**:

- актуальность — регулярная обновляемость;
- корректность — данные должны быть собраны из проверенных официальных источников или верифицированы активистами значимых сообществ, таких как Open Data Science.

Актуальные и востребованные источники открытых данных о пандемии COVID-19

Данные о ситуации с COVID-19 в России	<p>ежедневные отчеты Коммуникационного центра Правительства РФ по ситуации с коронавирусом сайта стопкоронавирус.рф</p> <p>ежедневные сводки Роспотребнадзора об актуальной эпидемической ситуации в России и мире</p> <p>данные карты индекса самоизоляции Яндекса: данные в JSON</p> <p>репозиторий с копией данных, предоставленных университетом Джонса Хопкинса, совмещенных с данными по России</p> <p>данные, собранные независимым аналитиком Сергеем Шпилькиным</p> <p>репозиторий доцента НИУ ВШЭ Алексея Куприянова для учета случаев эпидемии COVID-19 в России</p>
Данные о распространении COVID-19 в мире	<p>Novel Coronavirus (COVID-19) Cases, provided by JHU CSSE — официальные наборы данных от университета Джонса Хопкинса</p> <p>данные о случаях коронавируса от университета Джонса Хопкинса в JSON-формате</p> <p>Статистический отчет ЕС по COVID-19: Трекер COVID-19 для стран ЕС. Репозиторий: https://github.com/Jonur/covid19-eu-report</p> <p>Worldometers</p>

	Статистика и исследования COVID-19 от проекта “Our World in Data”
	Репозиторий наборов исторических данных, связанных с COVID-19
	Coronavirus (Covid-19) Data in the United States — сведения о распространении вируса и смертности в США от команды издания New York Times
	Обобщенные анонимные данные о перемещениях (мобильности) населения от Google по странам
	Apple Mobility Trends Reports (CSV)
	Набор данных о COVID-19 на Kaggle
	Corona Virus (COVID-19) Tweets Dataset — набор данных твитов о распространении коронавируса
Социально-экономические данные	Моделирование управления распространением заболеваний в регионах по данным о демографических/ экономических факторах
	International Monetary Fund’s COVID-19 Policy Tracker

Таблица составлена по материалам публикации на сайте covid19faq.ru

Проблемы открытых данных о COVID-19

Данные о COVID-19 относятся к категории чувствительных, поскольку результаты прогнозирования сценариев эпидемиологической ситуации вызывают общественный резонанс. Поэтому анализ этих данных требует аккуратности, а интерпретация результатов — ряда допущений, так как изначально таким данным присущи следующие особенности:

- Разрозненность источников и форматов данных. Отсутствие единой электронной таблицы, которую каждый заполняет в соответствии с единой методологией и которая легко позволила бы сравнить случаи заражения и смертности по всему миру.

- Большая разница между мерами профилактики и борьбы с коронавирусом и их несопоставимость по странам и городам, что влияет на данные и общее знание о том, сколько людей на самом деле заразились COVID-19¹⁷.

2.3. Робототехника и технологии

Новый коронавирус привел к росту практического интереса к роботам, беспилотным воздушным судам и искусственноому интеллекту. Задача технологий – справиться с массовой нехваткой кадров в здравоохранении, производстве и цепочках поставок, облегчить «социальное дистанцирование», диагностику и лечение, а также оптимизировать труд медиков и персонала, занимающегося дезинфекцией в очагах распространения возбудителя заболевания, обеспечивая при этом безопасность работы указанного персонала¹⁸.

2 апреля 2020 г. 30 ведущих мировых экспертов в области цифровых технологий собрались в формате круглого стола, чтобы обсудить возможности усиления реакции ВОЗ на COVID-19. Пандемия вызвала беспрецедентный спрос на цифровые технологии в области здравоохранения и выявила успешные решения, такие как скрининг населения, отслеживание инфекции, определение приоритетов в использовании и распределении ресурсов, разработка целевых ответных мер¹⁹.

Так, все большую популярность приобретают роботы-помощники в сфере здравоохранения.

В китайских больницах появились роботы-помощники. Они развозят лекарства больным, собирают мусор, постельное белье. В провинции Цзянсу на улицы вышли роботы на основе технологии 5G. Они самостоятельно передвигаются в местах массового скопления людей, распознают лица, дистанционно измеряют температуру, отслеживая одновременно до 32 человек²⁰. Более 30 дезинфекционных роботов, разработанных и изготовленных на шанхайском

¹⁷ <https://covid19faq.ru/l/ru/article/smrgcguuguh-hand-collected-coronavirus-data-sources>

¹⁸ <http://edurobots.ru/2020/03/covid-19-report/>

¹⁹ <https://www.who.int/news-room/detail/03-04-2020-digital-technology-for-covid-19-response>

²⁰ <https://vc.ru/tech/110577-it-tehnologii-v-borbe-s-koronavirusom>

предприятиях, использовались в крупных больницах Ухани – эпицентре вспышки коронавируса²¹. Похожие разработки применяются и в Индии²².

Литовский производитель робототехники Rubedo sistemas предлагает для массового производства робота-дезинфектора. Разработчики утверждают, что робот способен уничтожить в помещении 99% бактерий, вирусов и грибков²³.

Сингапурские ученые изобрели управляемого дистанционно при помощи ноутбука или планшета робота-уборщика, способного мыть и дезинфицировать труднодоступные поверхности – под столами и кроватями. Устройство проходит процесс тестирования в различных учреждениях и общественных местах²⁴.

В целях исключения риска передачи инфекции от зараженных пациентов медицинским работникам в государственной больнице колледжа Стенли в штате Тамилнад (Индия) в качестве эксперимента используют роботов для раздачи продуктов питания и лекарств²⁵.

Почти с самого начала распространения коронавируса большую популярность приобрели дроны.

На улицах китайских провинций появились дроны с громкоговорителями, также задействованы дроны-тепловизоры, которые могут определить температуру тела человека, находящегося даже на своем балконе, и сообщить данные в медучреждение. Дроны освещают строительные площадки, информируют население в отдаленных населенных пунктах о ситуации в стране, доставляют еду и многое другое²⁶. Китайские беспилотники, которые ранее использовались для распыления пестицидов в сельском хозяйстве, были адаптированы для распыления дезинфицирующих средств в местах скоплениях людей и в общественном транспорте. Для этих целей используются дроны XAG Technology. На фермах одно такое устройство покрывает 60 гектаров в час²⁷.

В Испании беспилотные летательные аппараты используются для дезинфекции улиц²⁸.

²¹ <https://global.chinadaily.com.cn/a/202002/07/WS5e3cfe0fa310128217275cd2.html>

²² <https://medicaldialogues.in/state-news/tamil-nadu/drones-used-to-spray-antiseptic-solution-around-covid-19-ward-at-madurai-government-hospital-64780>

²³ https://www.dp.ru/a/2020/03/26/Borba_ES_s_koronavirusom

²⁴ <https://www.thejakartapost.com/life/2020/04/17/singapore-disinfecting-robot-trialed-in-virus-fight.html>

²⁵ <https://medicaldialogues.in/state-news/tamil-nadu/robotic-nurses-to-deliver-drugs-to-covid-19-patients-in-tamil-nadu-hospital-64552>

²⁶ <https://vc.ru/tech/110577-it-tehnologii-v-borbe-s-koronavirusom>

²⁷ https://habr.com/ru/company/kauri_iot/blog/493302/

²⁸ <https://www.bbva.com/en/drones-to-stop-the-covid-19-epidemic/>

В Руанде дронов использует полиция, чтобы информировать население об ограничительных мерах в связи с коронавирусом, а также для выявления нарушителей карантина²⁹.

Технологии искусственного интеллекта также широко применяется в борьбе с коронавирусом.

В Китае в медучреждениях применяются системы анализа томограмм на основе искусственного интеллекта, что позволяет быстрее отличить обычную пневмонию от пневмонии, вызванной 2019-nCoV. Общественный транспорт в китайских городах оборудован умными термометрами и системами распознавания лица человека в маске³⁰.

В Австралии разработанная ранее компанией-стартапом DetectED-X для обнаружения онкологических заболеваний нейросеть может быть использована для диагностики коронавирусной инфекции COVID-19. Любое медучреждение в мире сможет бесплатно воспользоваться технологией, зарегистрировавшись на сайте разработчиков. Технология позволит врачам, анализирующими полученные в результате компьютерной томографии снимки легких, проверять диагноз в режиме реального времени³¹.

Компания Apple совместно с американским государственным Центром по контролю и предотвращению заболеваний (Centers for Disease Control and Prevention – CDC) и Федеральным агентством по управлению в чрезвычайных ситуациях запустили приложение, позволяющее проводить скрининг на наличие коронавируса. Анализируя ответы на различные вопросы, сформулированные на основе рекомендаций CDC, приложение подсказывает, какие действия следует предпринять, включая необходимость сдать тест на коронавирус, если пользователю показалось, что у него есть симптомы COVID-19. Приложение будет регулярно обновляться в соответствии с актуальными рекомендациями CDC. Кроме того, CDC предоставит все используемые в приложении алгоритмы в формате открытого кода для того, чтобы любые компании-разработчики могли использовать их при создании и усовершенствовании своих программ³².

Полицейским в Шанхае и некоторых других городах Китая выдали AR-шлемы (шлемы с использованием технологии дополненной реальности), разработкой занималась компания Kuang-Chi Technology. Гаджет позволяет за несколько секунд проверять температуру людей на расстоянии до 5 метров с

²⁹ <https://www.thestar.com.my/tech/tech-news/2020/04/18/covid-19-rwanda-uses-drones-to-help-catch-lockdown-transgressors>

³⁰ <https://vc.ru/tech/110577-it-tehnologii-v-borbe-s-koronavirusom>

³¹ <https://www.sydney.edu.au/news-opinion/news/2020/03/30/world-first-tool-to-improve-covid-19-diagnosis-free-and-online.html> <https://www.detectedx.com/>

³² <https://www.theverge.com/2020/3/27/21197056/apple-coronavirus-covid-19-website-app-online-screening-tool-cdc>

помощью инфракрасных камер. Если шлем показывает человека с повышенной температурой, включается аудио-оповещение. Также устройство оснащено камерой с алгоритмом распознавания лиц и считывания QR-кода. Информация о гражданине будет отображаться на виртуальном экране внутри шлема³³.

Инженеры и ученые ищут новые высокотехнологические способы разработки медицинских средств защиты. Один из вариантов решения проблемы нехватки медицинских масок – 3D печать.

Производитель материалов для 3D-печати Copper3D опубликовал цифровой файл STL с открытым исходным кодом респиратора N95 для печати в 3D-формате³⁴.

Когда в больнице города Брешиа (Италия) закончились дыхательные клапаны, необходимые для подключения пациентов к аппаратам ИВЛ, поставщик не смог оперативно удовлетворить внезапно возросший спрос. Для решения проблемы инженерная фирма Isinnova запустила 3D печать недостающих деталей³⁵.

Высший орган аудита (BOA) Чехии непосредственно участвует в борьбе с коронавирусом: BOA запущена печать медицинских масок на 3D-принтере³⁶.

2.4. Суперкомпьютеры и поиск методов лечения

В условиях пандемии COVID-19 правительства многих стран мира в тесном сотрудничестве с частными компаниями и научно-исследовательскими организациями активно применяют высокопроизводительные вычислительные системы – как традиционные суперкомпьютеры, так и технологии облачных (grid) вычислений, основывающихся на массовом использовании мощностей обычных компьютеров, объединенных в глобальную вычислительную сеть через стандартные протоколы передачи данных.

Доступ к высокопроизводительным вычислительным системам является критически важным для успешной реализации фундаментальных и прикладных молекулярно-генетических исследований возбудителя COVID-19, например, для изучения работы

³³ https://habr.com/ru/company/kauri_iot/blog/493302/

³⁴ <http://emag.medicalexpo.com/covid-19-3d-printed-face-masks-for-mass-screening/>

³⁵ <https://3dprintingindustry.com/news/3d-printing-community-responds-to-covid-19-and-coronavirus-resources-169143/>

³⁶ <https://www.nku.cz/cz/pro-media/tiskove-zpravy/prezident-nku-miloslav-kala:-svet-uz-nebude-stejny--a-az-vse-pomine--bude-cthit-odpovedi-id11121/>

молекул белка, участвующего в подавлении COVID-19 иммунной системой человека, разработке вакцин и противовирусных фармацевтических препаратов, эпидемиологического моделирования и многих других задач, в том числе с использованием технологий искусственного интеллекта и Big Data³⁷.

Один из успешных примеров такого государственно-частного партнерства – сформированный в США по инициативе Управления научно-технической политики Исполнительного офиса президента США, Министерства энергетики США и нескольких крупнейших американских ИТ-компаний Консорциум высокопроизводительных вычислений, связанных с COVID-19. Целью консорциума является координация предоставления вычислительных ресурсов для исследовательских программ, связанных с COVID-19, в том числе по поиску оптимальных методов лечения, молекулярно-генетическим исследованиям вируса и эпидемиологическому моделированию. По состоянию на 18 апреля 2020 г., в консорциуме участвует 31 организация: восемь ведущих американских корпораций (IBM, Amazon Web Services, AMD, BP, Google Cloud, Hewlett Packard Enterprise, Microsoft, NVIDIA), шесть национальных лабораторий Министерства энергетики США и девять академических лабораторий (включая Массачусетский технологический институт), НАСА, Национальный научный фонд и восемь крупнейших суперкомпьютерных центров страны, включая Национальный центр суперкомпьютерных приложений. Совокупная вычислительная мощность консорциума составляет около 418 петафлопс, им поддерживается 27 научно-исследовательских проектов³⁸.

1 петафлопс означает, что за секунду машина может совершить 1 000 000 000 000 (один квадриллион) операций с плавающей точкой. Это примерно в 50 000 больше, чем скорость обычного персонального компьютера³⁹.

Проект имеет и международное значение. С 22 марта 2020 г. консорциум получил 55 заявок на предоставление вычислительных мощностей от исследовательских центров

³⁷ <https://wikibon.com/breaking-analysis-big-data-in-the-fight-against-covid-19/>

³⁸ <https://covid19-hpc-consortium.org/>

³⁹ https://expert.ru/russian_reporter/2013/24/pomeryaemsya-petaflopsami_1/

не только из США, но и из Великобритании, Германии, Индии, Испании, Саудовской Аравии, Хорватии и ЮАР⁴⁰.

Национальная координация использования вычислительных мощностей суперкомпьютеров в интересах борьбы с COVID-19 в рамках частно-государственного партнерства осуществляется в Германии⁴¹ и других государствах – членах Европейского союза (в том числе и при финансовой поддержке Европейской комиссии в рамках проекта EXSCALEATE4CoV)⁴², Сингапура⁴³ и других странах мира.

На исследования COVID-19 были перепрофилированы и многие международные проекты облачных вычислений, наиболее масштабным из которых является проект folding@home, созданный в 2000 г. под эгидой Стэнфордского университета (США) для проведения компьютерного моделирования свертывания молекул белка при различных наследственных, онкологических и других заболеваниях, с текущей совокупной вычислительной мощностью $1,5 \times 10^{18}$ экзафлопс ($1,5 \times 10^{18}$ операций в секунду). В том числе с использованием суперкомпьютеров.

Венгерский суперкомпьютер SuperDome используется в рамках исследований COVID-19 Стэнфордского университета и участвует в международный проект folding@home. С его помощью проводятся симуляции, которые позволяют лучше понять работу ферментов, расщепляющих белки внутри вируса, и разработать ингибитор⁴⁴.

По состоянию на 18 апреля 2020 г., вычислительные мощности folding@home используются в целом ряде проектов, связанных с биологией возбудителя COVID-19, реализуемых 11 лабораториями в разных странах мира⁴⁵.

Примеры использования суперкомпьютеров для борьбы с COVID-19 есть и в России.

Сколковский институт науки и технологий предоставит мощности суперкомпьютера «Жорес» для исследования COVID-19.⁴⁶ А МГУ – мощности

⁴⁰ <https://www.wsj.com/articles/supercomputers-help-researchers-speed-drug-discovery-for-covid-19-11586888735>

⁴¹ <https://prace-ri.eu/eu-hpc-fights-covid-19/#JointInternationalInitiatives>

⁴² <https://www.excalate.eu/en/projects.html#Covid-19>

⁴³ <https://www.asianscientist.com/2020/03/tech/nscc-covid-19-special-call-for-projects/>

⁴⁴ <http://abouthungary.hu/news-in-brief/coronavirus-heres-the-latest/>

⁴⁵ <https://foldingathome.org/covid19/>

⁴⁶ <https://www.skoltech.ru/2020/03/skoltech-gotov-predostavit-resursy-superkompyutera-zhores-dlya-borby-s-pandemiej-koronavirusa/>

суперкомпьютера «Ломоносов» для молекулярного моделирования при разработке лекарственных препаратов против COVID-19⁴⁷.

Цифровые платформы также предпринимают шаги, направленные на поддержку усилий по поиску новых методов лечения COVID-19. Например, в Китае Alibaba Cloud объявил о бесплатном доступе к возможностям искусственного интеллекта с целью научных разработок новых лекарств и вакцин от вируса.

2.5. Новые технологические стартапы

В целях поиска новых методов борьбы с COVID-19 во многих странах запущены государственные программы отбора и финансирования стартапов, предлагающих инновационные разработки в области диагностирования и лечения нового коронавируса, а также решения сопутствующих проблем.

Правительство Германии провело специализированный [хакатон](#), который привлек 42 тысячи участников и более 800 проектов.

Стартап компании DOCYET создал онлайн-чат-бота, который анализирует данные о физиологических показателях пользователя, проводит оценку рисков и предлагает варианты для удаленных консультаций. При этом, Министерство здравоохранения запустило «Инновационный хаб в области здоровья», на котором среди прочего размещены проверенные сервисы для удаленных медицинских консультаций, большинство из которых бесплатны⁴⁸.

Британское космическое агентство при участии Европейского космического агентства создало фонд в размере 2,6 млн фунтов стерлингов (3,26 млн долл. США) с целью финансирования проектов и стартапов, применяющих высокотехнологичные разработки и достижения космической промышленности для решения наиболее актуальных проблем национальной системы здравоохранения в условиях пандемии, таких как использование дронов для доставки диагностических тестов и медицинских средств индивидуальной защиты либо использование спутниковых данных для контроля вспышек заболеваемости.

⁴⁷ <https://ria.ru/20200407/1569684905.html>

⁴⁸ <https://medicalfuturist.com/how-germany-leveraged-digital-health-to-combat-covid-19/>

Проекты, претендующие на финансирование, могут использовать спутниковые коммуникации и навигацию, технологии спутникового мониторинга земной поверхности, а также любые другие технологии, связанные с полетами человека в космос. Некоторые разработки уже используются, например, при контроле соблюдения социального дистанцирования с использованием спутниковых данных GPS и искусственного интеллекта⁴⁹.

Одним из основных проблемных моментов для ученых при разработке методов диагностики и лечения, а также вакцин, является недостаточно оперативный поиск подходящих кандидатов для тестирования, из-за чего, как показывает практика, срываются сроки испытаний в 86% случаев. Новая цифровая платформа «Мир без коронавируса» ([World Without COVID](#)), запущенная в США, призвана найти пациентов-добровольцев для клинических испытаний⁵⁰.

Институтом клинических исследований Университета Дьюка (США) запущена онлайн-платформа, на которой на добровольной основе собирается информация от медицинских работников, непосредственно участвующих в лечении зараженных пациентов и борьбе с последствиями коронавируса, с целью создания качественной базы данных об эффективных мерах предосторожности и способах защиты медицинского персонала, о влиянии COVID-19 на пациентов, о ходе испытаний лекарств и методов лечения. Преимуществом такого подхода является открытость и масштабность, поскольку ранее полученные данные по этим вопросам не имеют никакого подтверждения либо основаны на ограниченных исследованиях⁵¹.

3. Дистанционная работа и образование

⁴⁹ British space industry joins race to help NHS deal with coronavirus / <https://www.mobihealthnews.com/news/europe/british-space-industry-joins-race-help-nhs-deal-coronavirus>

⁵⁰ As researchers rush for COVID-19 cure, new platform seeks to help link patients with clinical trials / <https://www.mobihealthnews.com/news/researchers-rush-covid-19-cure-new-platform-seeks-help-link-patients-clinical-trials>

⁵¹ <https://www.healthcareitnews.com/news/new-duke-registry-invites-hospital-workers-share-data-covid-19>

3.1. Адаптация к цифровому формату трудовой деятельности

По оценкам Международной организации труда, полные или частичные ограничительные меры в связи с пандемией коронавирусной инфекции уже затрагивают 2,7 млрд трудящихся или 81% от всей рабочей силы во всем мире, что приводит к вынужденному сокращению занятости как в форме увольнений работников, так и сокращения оплачиваемого рабочего времени. Во 2-м квартале 2020 г. ожидается сокращение оплачиваемых рабочих часов на 6,7%, что эквивалентно 195 млн рабочих мест.

При этом, с точки зрения общего сокращения оплачиваемого рабочего времени, наименьший эффект пандемии на занятость прогнозируется в Африканском регионе (сокращение на 4,9%), в то время как наибольший – в арабских государствах (сокращение на 8,1%).

Однако, на фоне сокращения спроса на рабочую силу во многих отраслях экономики наметились несколько сфер, где потребность в новых сотрудниках, наоборот, увеличилась. Так, производители программного обеспечения для удаленной командной работы (Zoom, Slack) размещают вакансии по всем направлениям, включая программирование, бухгалтерию, продажи и поддержка клиентов, а онлайн-сервис Support.com объявил неограниченный набор на должности удаленной технической поддержки в связи с резким ростом звонков и обращений, поскольку, как оказалось, немногие пользователи, вынужденные работать удаленно, обладают необходимыми техническими навыками⁵².

Тем не менее использование технологий при поиске работы в условиях пандемии COVID-19 стало вынужденным социальным экспериментом в области дистанционного управления, поскольку, например, до 50% всех работающих граждан в США в настоящее время работают удаленно, что более чем вдвое превышает показатели 2017–2018 гг. И если, с одной стороны, такой режим работы сокращает вредные выбросы и офисные расходы и способствует возможности совмещения рабочих и семейных обязанностей, то его обратной стороной является негативный эффект на продуктивность управления персоналом и профессиональный рост работников. Если

⁵² <https://www.forbes.com/sites/ashleystahl/2020/04/01/4-industries-who-are-still-hiring-in-the-midst-of-covid-19/#78d681c615ee>

новая культура дистанционного общения приживется, пандемия значительно ускорит ранее наметившуюся тенденцию к активизации удаленной работы⁵³.

До пандемии около 70% компаний уже работали в направлении цифровой трансформации своего бизнеса, в рамках которой возможность удаленной работы стоит наравне с такими ключевыми элементами, как доставка товаров, проведение виртуальных мероприятий и использование облачных технологий. При этом, согласно исследованию Harvard Business Review, из 1,3 трлн долл. США, потраченных компаниями на цифровую трансформацию в 2018 г., примерно 900 млрд долл. США были потрачены впустую, так как реализованные инициативы не принесли желаемого результата. В этой связи многие компании не хотели идти на риск цифровизации, хотя и боялись потерять долю на рынке. Пандемия COVID-19, безусловно, внесет корректировки в эти планы⁵⁴.

3.2. Онлайн-обучение: перспективы и вызовы

Кризис, вызванный распространением COVID-19, будет способствовать переходу к «цифровому капитализму» во многих сферах жизнедеятельности. Однако, [по мнению экспертов ОЭСР](#), данный тренд может не затронуть сферу образования.

Образование по-прежнему не ассоциируется со сферой заметного получения прибыли. По крайне мере в сравнении со здравоохранением, где изобретается и производится множество новых лекарств и технологий лечения. По оценкам ОЭСР⁵⁵, капитализация сферы здравоохранения (рыночная стоимость компаний) представляет около 50% от всего объема средств, потраченных во всем мире на здравоохранение (5 из 10 трлн долл. США). В сфере образования эта цифра меньше 2% (0,15 из 6 трлн долл. США). Поэтому возникают опасения, что инвестиции в сферу образования могут оказаться недостаточными для разработки средств и ресурсов, которые будут способствовать ее улучшению.

⁵³ <https://www.brookings.edu/blog/up-front/2020/04/06/telecommuting-will-likely-continue-long-after-the-pandemic/>

⁵⁴ <https://www.forbes.com/sites/blakemorgan/2020/04/05/is-covid-19-forcing-your-digital-transformation-12-steps-to-move-faster/#3bb19d50617b>

⁵⁵ В статье упоминается анализ данных различных источников (ВОЗ, HolonIQ, Goldman Sachs, Standard & Poors).

Тем не менее, в связи с коронавирусом сфера образования уже претерпела значительные изменения в силу перехода образовательных учреждений многих стран на дистанционный формат обучения. Учащиеся и учителя стремятся использовать современные технологические возможности. Например, [по данным ВЭФ](#), студенты в Гонконге перешли на дистанционное обучение при помощи интерактивных приложений, а в Китае доступ к образовательным ресурсам для 120 млн граждан осуществляется в том числе через прямые трансляции по телевидению. Подробный список цифровых образовательных платформ, используемых в разных странах, опубликован [на сайте ЮНЕСКО](#).

В одной из школ Нигерии стандартные несинхронные средства обучения (например, чтение с использованием Google Classroom) были дополнены синхронными инструкциями «лицом к лицу» по видео.

Учащиеся в Ливане «посещают» уроки физкультуры онлайн: они записывают и отправляют видео своих тренировок учителям в качестве домашнего задания. Тем не менее, с технической точки зрения процесс пока не оптимизирован. Родители одного из учеников [сообщили](#), что занятия спортом занимают несколько минут, тогда как на процесс записи, обработки и отправки видео требуется дополнительное время.

Наблюдается **усиление государственно-частного сотрудничества по вопросам образования**. За несколько недель сформировались образовательные консорциумы с участием различных стейкхолдеров, включая правительства, издательства, педагогов, разработчиков и поставщиков технологий и операторов телекоммуникационных сетей. Их целью стало предоставление временных технологических решений, в том числе, для сферы образования.

Министерство образования Китая пришло к соглашению с разными стейкхолдерами по поводу разработки новой программы обучения на основе использования облачных технологий, а также по поводу модернизации комплекса образовательной инфраструктуры.

Схожая ситуация произошла в Гонконге с форумом [readtogether.hk](#), который представляет консорциум более 60 образовательных организаций, издателей, СМИ и профессионалов индустрии развлечений. Консорциум намерен продолжать использовать и поддерживать платформу даже после того,

*как проблема
COVID-19 будет преодолена⁵⁶.*

Вместе с тем по мере вынужденного перехода к онлайн-обучению все более очевидными становятся масштабы цифрового разрыва и непропорционально большого числа школьников, не имеющих домашнего широкополосного доступа в Интернет. [По оценкам Федеральной комиссии по связи США \(FCC\)](#), в 2019 г. более 21,3 млн американцев не имели доступа к Интернету, особенно в сельских областях, что даже привело к возникновению такого понятия, как «разрыв в выполнении домашнего задания» (англ. – *homework gap*), когда учащиеся с более низкими доходами отстают от своих более обеспеченных одноклассников именно по причине невозможности выполнения части заданий в онлайн-формате. Учитывая приоритет сферы образования в современном обществе, по мере осознания и изучения последствий влияния пандемии COVID-19 на глобальные процессы, устранению цифрового разрыва в школьном образовании должно быть уделено первоочередное внимание⁵⁷.

Другим проблемным вопросом цифровизации образования стала подготовленность самих преподавателей к новому формату и необходимость их обучения. Так, в Европе и Южной Азии 50% государств проводят инструктаж учителей по вопросам дистанционного взаимодействия со студентами во время кризиса. В то же время в Африке к югу от Сахары треть государств ввели дистанционное обучение, однако ни одна из них не проводит тренинги в данном направлении⁵⁸.

[По мнению экспертов ВЭФ](#), в будущем использование новых технологий, особенно в области 5G, сделает возможным реализацию концепции «обучение где угодно, в любое время» (англ. – *learning anywhere, anytime*) в разных форматах. Традиционные виды обучения в классах будут дополнены новыми методами – от прямых эфиров до виртуальной реальности. Обучение может стать привычкой, которая интегрирована в обычную жизнедеятельность.

⁵⁶ 3 ways the coronavirus pandemic could reshape education / сайт ВЭФ / <https://www.weforum.org/agenda/2020/03/3-ways-coronavirus-is-reshaping-education-and-what-changes-might-be-here-to-stay>

⁵⁷ <https://www.brookings.edu/blog/techtank/2020/03/17/what-the-coronavirus-reveals-about-the-digital-divide-between-schools-and-communities/>

⁵⁸ <https://www.brookings.edu/research/school-closures-government-responses-and-learning-inequality-around-the-world-during-covid-19/>

ОЭСР [видит](#) три сценарии развития ситуаций после преодоления кризиса COVID-19. Первый предполагает возвращение к докризисным временам, насколько это будет возможно. Второй сценарий рассматривает тренды через призму суверенитета: будут ли страны готовы использовать сервисы и инструменты онлайн-обучения, которые предоставляются компаниями из ограниченного круга стран (учитывая, что крупнейшие мировые цифровые платформы расположены в США и Китае). Третий сценарий рассматривает кризис как новую возможность для международного сотрудничества. Более тесная кооперация – как между компаниями, так и в рамках международного государственно-частного партнерства – может помочь создать более доступные цифровые средства для обучения. Именно такой подход востребован в сфере здравоохранения для поиска быстрого решения проблемы коронавируса.

Информацию о применении цифровых технологий в сфере дистанционного обучения можно также найти в [дайджесте «Эпидемия коронавируса: воздействие на сферу образования»](#).

II. Риски и угрозы цифровому развитию

Вспышка коронавируса вынудила многих людей по всему миру работать и учиться дома, а предприятия и учреждения – переводить свою деятельность в онлайн-среду. Киберпреступники активно используют эти непростые обстоятельства, чтобы найти новые незаконные способы заработка. Они расширяют и диверсифицируют свою деятельность, пользуясь атмосферой страха и неопределенности⁵⁹.

В связи с этим в текущих условиях еще больше обозначилась потребность в международном сотрудничестве по противодействию такого рода преступлениям. Различия стран в подходах к регулированию виртуального пространства не должны быть препятствием в совместной работе.

[Доктрина информационной безопасности Российской Федерации](#) (утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. №646) дает следующее определение информационной безопасности. Это состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация прав и свобод человека и гражданина,

⁵⁹ COVID-19 crimes / Сайт Интерпола / <https://www.interpol.int/How-we-work/COVID-19>

достойные качество и уровень жизни граждан; безопасность в информационной сфере. Под информационной сферой понимается 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.

В более узком смысле трактуется в западных странах (прежде всего США, Великобритания) безопасность виртуальной среды как состояние защищенности сетей, компьютеров, программ и данных от взлома, повреждений или несанкционированного доступа. Для этих целей чаще всего используется понятие **кибербезопасности** («cyber» – «связанный с компьютерами и Интернетом»). Одна из ключевых характеристик кибербезопасности – быстрый и постоянно эволюционирующий характер угроз. В стремительно меняющемся мире в период пандемии COVID-19 это проявляется особенно четко.

Международные организации (Интерпол, Европол, Еврокомиссия, Группа реагирования на компьютерные инциденты в рамках институтов, учреждений и органов Европейского союза – CERT-EU) в контакте друг с другом отслеживают преступную деятельность в киберпространстве, повышают осведомленность лиц, принимающих политические решения, а также граждан, и готовы координировать свои действия в случае необходимости.

1. Факторы, влияющие на кибербезопасность

Европол (Агентство по сотрудничеству правоохранительных органов Европейского союза) [выделяет основные факторы](#), которые влияют на уровень киберпреступности:

- высокий спрос на определенные товары, защитные средства и фармацевтическую продукцию;
- снижение мобильности граждан;
- граждане остаются дома и все чаще работают на дому, используя цифровые решения;
- ограничения в общественной жизни делают некоторые преступные действия менее заметными и переносят их в онлайн-пространство;

- увеличение уровня тревожности в обществе;
- сокращение поставок определенных товаров.

2. Глобальные угрозы

В связи с тем, что COVID-19 меняет ситуацию в правоохранительной сфере, Интерпол (Международная организация уголовной полиции) опубликовал оценку глобальной угрозы преступности и полицейской деятельности для своих 194 стран-членов. [Доклад](#), предназначенный только для правоохранительных органов, опирается на экспертные знания и будет регулярно обновляться по мере появления новых угроз. В нем описывается «жизненный цикл преступности», а также лучшие практики и меры по смягчению последствий преступлений, связанных с COVID-19.

В частности, отмечается, что виды преступлений постоянно эволюционируют, используя особенности онлайн-поведения и новых потребностей граждан в условиях эпидемии COVID-19. Поскольку одна треть населения мира в настоящее время находится в той или иной форме изоляции, изменения в структуре преступности уже дали о себе знать⁶⁰. Число домашних краж со взломом заметно сократилось, но воры все чаще выбирают фабрики или служебные помещения, которые стоят пустыми.

В докладе Интерпола указаны **глобальные угрозы**, вызванные COVID-19, в том числе в сфере кибербезопасности (представлены далее).

2.1. Кибератаки: вредоносные домены, вредоносные программы и вымогательство в сети

- **Вредоносные домены.** Киберпреступники каждый день создают тысячи сайтов, которые содержат слова «коронавирус», «COVID-19», различные вариации написания

⁶⁰ Preventing crime and protecting police: Interpol's COVID-19 global threat assessment/ Сайт Интерпола / <https://www.interpol.int/en/News-and-Events/News/2020/Preventing-crime-and-protecting-police-INTERPOL-s-COVID-19-global-threat-assessment>

этих терминов и используют их для проведения спам-кампаний⁶¹, фишинга⁶², распространения вредоносных программ или взлома серверов управления и контроля.

- **Вредоносное программное обеспечение (ПО).** Киберпреступники пользуются популярностью сообщений о коронавирусе для маскировки своей деятельности. Вредоносные, шпионские и троянские вирусные программы⁶³ обычно представлены под видом интерактивных карт и веб-сайтов о коронавирусе. Спам-сообщения также заставляют пользователей переходить по ссылкам, которые загружают вредоносное ПО на компьютеры или мобильные устройства.

Всемирная организация здравоохранения [заявила](#), что хакеры и кибермошенники используют пандемию коронавируса, отправляя фишинговые сообщения посредством электронной почты и мессенджеров якобы от имени организации. С их помощью злоумышленники могут установить вредоносное ПО или украдь конфиденциальную информацию.

- **Вымогательство.** Киберпреступники подвергают серверы больниц, медицинских центров и государственных учреждений атакам и вымогательству. Учреждения, находящиеся на переднем крае борьбы с коронавирусом, сталкивающиеся с беспрецедентной опасностью для здоровья, теперь также противостоят еще одной угрозе – со стороны киберпреступников. Их доступ к жизненно важным файлам и системам оказывается заблокированным до тех пор, пока не будет выплачен выкуп. Поскольку в условиях кризиса в области здравоохранения больницы не могут позволить, чтобы их системы были заблокированы, они вынуждены платить преступникам. Блокирование работы больниц и их критических систем не только задерживает оперативную медицинскую деятельность, столь необходимую в период пандемии, но и может непосредственно привести к смертельным случаям.

Программа-вымогатель может проникнуть в системы через электронные письма, скомпрометированные учетные данные сотрудников или с помощью уязвимости в системе.

⁶¹ Спам – массовая рассылка корреспонденции рекламного характера лицам, не выражавшим согласия ее получать.

⁶² Фишинг – это разновидность интернет-мошенничества, совокупность методов, позволяющих обмануть пользователя и заставить его раскрыть свой пароль, номер кредитной карты и другую конфиденциальную информацию.

⁶³ Троянская вирусная программа (также троян) – разновидность вредоносной программы, проникающая в компьютер под видом легитимного программного обеспечения, в отличие от других вирусов, которые распространяются самопроизвольно.

13 апреля 2020 г. совершена кибератака, направленная на университетскую больницу Брно в Чешской Республике. Это вынудило медиков отложить операции и направить пациентов с острыми заболеваниями в ближайшую клинику⁶⁴.

Киберпреступники, вероятно, будут стремиться использовать все большее число новых способов атак, поскольку все больше работодателей вводят дистанционный режим работы и устанавливают удаленное подключение к своим системам для сотрудников.

2.2. Мошенничество и контрафактная торговля средствами индивидуальной защиты и противовирусными лекарственными средствами

Помимо исключительно «цифровых» преступлений на фоне пандемии обостряются и ранее существовавшие проблемы, которые перешли в электронный формат. Злоумышленники очень быстро адаптировали известные схемы мошенничества к новым условиям, чтобы извлечь выгоду из кризиса, связанного с пандемией COVID-19.

- Продажа через Интернет контрафактной медицинской продукции⁶⁵. Поскольку спрос на средства индивидуальной защиты и гигиены растет в геометрической прогрессии, преступники стремятся получить прибыль, продавая некачественные или контрафактные товары, такие как хирургические маски, дезинфицирующие средства, противовирусные и противомалярийные препараты (включая несуществующие лекарства от COVID-19), вакцины, тест-наборы для анализа на коронавирус.

Некачественные защитные маски и дезинфицирующие средства, нелегальные противовирусные препараты были изъяты в рамках операции «Лангея XIII» в марте 2020 г., в ходе которой полиция, таможня и органы здравоохранения 90 стран приняли участие в коллективных действиях против незаконной продажи лекарств и медицинских товаров в Интернете. В ходе операции был арестован 121 подозреваемый по всему миру, а также проведено изъятие потенциально опасных фармацевтических препаратов на сумму более 14 млн долл. США⁶⁶.

⁶⁴ How criminals profit from the COVID-19 pandemic / Сайт Европола /

<https://www.europol.europa.eu/newsroom/news/how-criminals-profit-covid-19-pandemic>

⁶⁵ Fake medicines / Сайт Интерпола / <https://www.interpol.int/en/Crimes/Illicit-goods/Shop-safely/Fake-medicines>

⁶⁶ Global operation sees a rise in fake medical products related to COVID-19 / Сайт Интерпола / <https://www.interpol.int/en/News-and-Events/News/2020/Global-operation-sees-a-rise-in-fake-medical-products-related-to-COVID-19>

- **Финансовое мошенничество.** Поскольку хирургические маски и другие медицинские принадлежности пользуются большим спросом, но их трудно найти в розничных магазинах, в Интернете появились поддельные магазины, веб-сайты, учетные записи в социальных сетях, якобы торгующие этими товарами. Но после перечисления оплаты товары покупателю не отправляются.

Интерпол оказал помощь в выявлении 30 случаев мошенничества, связанных с COVID-19 в Азии и Европе, что привело к блокировке 18 банковских счетов мошенников и заморозке более 730 тыс. долл. США. Интерпол также выпустил [уведомление](#), предупреждающее полицию во всех 194 странах-членах об этом виде преступлений.

Европол также сообщает о новом способе мошенничества. Во многих странах правительства выделяют прямую финансовую помощь, чтобы содействовать гражданам в преодолении последствий экономического кризиса, вызванного пандемией. Но многие программы еще не полностью отлажены, и граждане не могут понять, как к ним подключиться. Мошенничество направлено на получение банковских реквизитов граждан.

В Канаде рассыпались мошеннические текстовые сообщения, обещавшие связать получателей с государственными фондами⁶⁷.

2.3. Информационные угрозы в эпоху COVID-19

В последние недели, по данным Интерпола, возросла онлайн-активность педофилов, которые ищут материалы о сексуальном насилии над детьми, что усугубляется нехваткой модераторов, которые могли бы выявлять и удалять оскорбительные материалы из сети Интернет.

По мере роста использования социальных сетей (Twitter, Facebook, Wechat) в качестве средства получения информации, а также для сохранения контактов с родственниками, друзьями и коллегами в отсутствии возможности физического общения. В Китае были созданы тысячи групп на платформе WeChat, чтобы связать людей, способных помочь, с теми, кто нуждается в помощи.

⁶⁷ Cybercrime spikes during coronavirus pandemic, says Europol / Сайт Европьюс / <https://www.euronews.com/2020/03/27/cybercrime-spikes-during-coronavirus-pandemic-says-europol>

В то время как социальные сети полезны для обмена информацией, они также становятся **источником «фейковых новостей»**. Компании стараются предпринимать усилия для борьбы с негативным феноменом⁶⁸.

Возможными оправданными выходами из такой ситуации могут стать как соблюдение «социального медиа дистанцирования», предполагающее добровольное сокращение использования социальных сетей в качестве источников информации, так и внедрение ведущими социальными платформами системы проверки фактов и блокирования непрошедших проверку сообщений⁶⁹. Например, мессенджер WhatsApp уже ограничил пересылку сообщений до одного раза из-за угрозы фейков о COVID-19⁷⁰. Крупнейшие американские интернет-компании и соцсети (Google, Facebook, Twitter) объявили о совместных действиях, направленных на борьбу с дезинформацией о COVID-19⁷¹.

Отдельный вид угроз связан с возрастающей нагрузкой на цифровые сервисы и технологии. Так, вместе со стремительным ростом аудитории некоторые сервисы столкнулись со **сложностями, вызванными резким увеличением нагрузки на их технологические возможности**.

Youtube снизил качество показа видео с HD до «стандартного». При этом пользователи по-прежнему смогут регулировать настройки вручную. Netflix также понизил разрешение видео с целью сокращения трафика⁷².

В этой связи Брукингский институт обращает внимание на то, что глобальный Интернет столкнулся с **беспрецедентным ростом трафика** в условиях масштабного перехода населения к удаленной работе и обучению, однако его пропускная способность пока смогла удовлетворить все возросшие потребности. Отчасти это объясняется тем, что максимальная производительность каналов связи была рассчитана и подготовлена таким образом, чтобы удовлетворять массовое использование сервисов потокового видео типа Netflix в пиковые вечерние часы.

⁶⁸ The COVID-19 Crisis: Accentuating the Need to Bridge Digital Divides / Сайт ЮНКТАД / https://unctad.org/en/PublicationsLibrary/dtlinf2020d1_en.pdf

⁶⁹ Бхаксар Чакроворти, приглашенный старший исследователь отделения Брукингского института в Индии. <https://indianexpress.com/article/opinion/columns/social-media-distancing-coronavirus-fake-news-bhaskar-chakravorti-6350425/>

⁷⁰ WhatsApp ограничил пересылку сообщений до одного раза из-за угрозы фейков о COVID-19 / Сайт Интерфакс / <https://www.interfax.ru/world/702974>

⁷¹ Google, Facebook и Twitter объявили о совместной борьбе с фейками о коронавирусе / Сайт Новой газеты / <https://novayagazeta.ru/news/2020/03/17/159857-google-facebook-i-twitter-ob-yavili-o-sovmestnoy-borbe-s-feykami-o-koronaviruse>

⁷² Эхо карантина: Netflix и Youtube снизили разрешение видео в ЕС / Сайт Gazeta.ru / https://www.gazeta.ru/culture/2020/03/20/a_13014301.shtml

Однако в технологическом плане пропускная способность Интернета не безгранична, что может представлять угрозу в случае неблагоприятного дальнейшего развития ситуации⁷³.

3. Принимаемые меры

3.1. Взаимодействие на государственном уровне.

Интерпол помогает странам-членам расследовать кибернападения на больницы и смягчать их последствия. Чтобы поддержать глобальные усилия по борьбе с этой критической опасностью, организация выпустила уведомление, предупреждающее полицию всех 194 стран-членов об усилении угрозы кибервымогательства.

Кроме того, Интерпол формирует список подозрительных интернет-доменов, связанных с COVID-19, проводит их дальнейший анализ и оценку, и взаимодействует с соответствующими странами для принятия мер.

Интерпол работает круглосуточно, поддерживая сотрудников полиции в странах-членах организации, поскольку они сталкиваются с беспрецедентными проблемами. Взаимодействие осуществляется посредством безопасной глобальной системы связи, а также системы уведомлений с цветовой кодировкой, которая позволяет странам всего мира обмениваться предупреждениями и запросами информации. Опубликованы [международные руководящие принципы в целях повышения безопасности и эффективности правоохранительных органов и оказания помощи в контексте пандемии COVID-19](#).

3.2. Взаимодействие с частными партнерами.

Группа реагирования на угрозы киберпреступности Интерпола следит за всеми киберугрозами, связанными с COVID-19, тесно сотрудничая с частными партнерами в отрасли кибербезопасности, чтобы собирать информацию и оказывать поддержку организациям.

⁷³ <https://www.brookings.edu/blog/techtank/2020/04/02/why-the-internet-didnt-break/>

3.3. Помощь пострадавшим сторонам.

Интерпол оказывает помощь, необходимую для обеспечения того, чтобы жизненно важные системы здравоохранения продолжали функционировать, вплоть до непосредственной технической поддержки, а также консультаций по вопросам смягчения последствий и защиты критически важной медицинской инфраструктуры⁷⁴.

3.4. Взаимодействие с гражданами.

Организация дает [общие рекомендации](#) и советы по профилактике киберугрозы для граждан.

В рамках операции «Пангея XIII» была проведена широкая информационная кампания посредством распространения видеороликов, брошюр, проведения выставок и бесед в больницах и школах для повышения осведомленности об опасности приобретения фармацевтических препаратов из нерегулируемых онлайн-источников.

3.5. Меры профилактики.

Группа реагирования на компьютерные инциденты в рамках институтов, учреждений и органов Европейского союза (CERT-EU) принимает меры для оценки цифровых аспектов коронавирусной пандемии. Группа включает экспертов по информационной безопасности из основных учреждений ЕС. CERT-EU сотрудничает с аналогичными учреждениями в государствах-членах и со специализированными компаниями в области информационной безопасности с целью реагирования на инциденты информационной безопасности и киберугрозы. Она [разработала план](#) устранения любой потенциальной угрозы, которая может повлиять на кибербезопасность и интересы институтов, учреждений и органов ЕС: «Гид по кибербезопасности: как пережить пандемию COVID-19». Гид описывает картину киберугроз и дает перечень конкретных мер, которые могут помочь предприятиям и учреждениям преодолеть кризис и предотвратить последствия кибератак:

⁷⁴ Cybercriminals targeting critical healthcare institutions with ransomware / Сайт Интерпол / <https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-health-care-institutions-with-ransomware>

1. Установить связь

- 1.1. Установить четкие внутренние каналы связи между инфраструктурой, группой безопасности и руководством и регулярно контролировать их. Определить безопасные резервные каналы связи, если существующие ИТ-системы, используемые для этой цели, недоступны.
- 1.2. Узнать о способах связи с государственной группой реагирования на инциденты в области компьютерной безопасности.
- 1.3. Убедиться, что имеется доступ ко всем средствам связи с государственной группой реагирования на инциденты в области компьютерной безопасности, чтобы сократить время отклика и повысить эффективность.

2. Определить соответствующих стейкхолдеров:

- 2.1. В своей организации.
- 2.2. В своем секторе предпринимательства.
- 2.3. Включить государственную группу реагирования в свой план реагирования на кризис.

3. Установить процесс реагирования на инциденты

- 3.1. Установить внутренний процесс реагирования на инциденты, включая процедуры, ключевых сотрудников и инструменты, которые позволили бы осуществлять этот процесс.
- 3.2. Знать о любых возможных каскадных последствиях нарушения кибербезопасности.
- 3.3. Ознакомиться с механизмами сообщения об инцидентах государственной группы реагирования.

Во время пандемии COVID-19 преступники активно используют возможности, которые им предоставил кризис, умело адаптируя свои методы. Угроза киберпреступности во время кризиса носит динамичный характер и имеет потенциал для дальнейшего разрастания. Учитывая беспрецедентное количество людей, которые постоянно находятся дома и пользуются онлайн-услугами, возможности преступников значительно возросли.

Ситуация усложняется тем, что многие вопросы взаимодействия в цифровой среде еще не до конца урегулированы в правовом поле. Это создает преступникам пространство для изобретения новых способов мошенничества.

Пандемия выявила уязвимости в устаревших системах безопасности как в компьютерах граждан, так и в системах предприятий и учреждений и потребовала от правительства принятия согласованных мер на государственном и международном уровнях.

III. Выводы и рекомендации

Пандемия коронавируса дала мощный импульс массовому внедрению цифровых технологий в повседневную жизнь. Уже сейчас очевидно, что перемены, которые эта тенденция внесет в общественно-экономический уклад, будут носить беспрецедентный характер.

Продолжающиеся в большинстве стран мира мероприятия по социальной изоляции заставили перейти в онлайн существенную часть мировой торговли товарами и услугами. Вероятно, в скором времени мир будет наблюдать дальнейший взрывной рост капитализации поставщиков онлайн-услуг на фоне падения позиций компаний сырьевых отраслей. Кардинально изменятся модели потребления. Заметная доля работы и образования также уйдет в дистанционный формат.

С одной стороны, эти изменения сделают жизнь человека еще более удобной. Широкие горизонты для развития человечества открывает возможность, не выходя из дома, обеспечивать себя необходимыми потребностями, задействовать для выполнения ряда «непrestижных» или опасных задач робототехнику, получать необходимую информацию об основных социально-экономических тенденциях в формате открытых данных, лечить заболевания и противодействовать их распространению с помощью технологий дистанционного взаимодействия, использования искусственного интеллекта и анализа больших данных.

Тем не менее существует огромный набор рисков и вопросов, на которые пока нет однозначного ответа. Как обеспечить приватность и защиту персональных данных в условиях активной цифровизации жизни? Как обеспечить права и свободы, поддержание которых стала едва ли не центральной скрепляющей идеологией для всего мира на протяжении второй половины XX века, когда передвижения граждан столько жестко фиксируются и регулируются в рамках мероприятий по изоляции? Как решить комплекс проблем, связанных с кибербезопасностью при том, что все большая часть нашей повседневной жизни будет переведена в онлайн-режим? Как преодолеть

неравенство возможностей в плане доступа к качественным онлайн-услугам в разных странах и социальных группах? Как изменится рынок труда и не возникнет ли проблема массовой безработицы в силу того, что многие профессии окажутся невостребованными в цифровую эпоху?

Можно ли считать скепсис противников цифровизации оправданным или же стоит воспринимать его как безосновательный неолуддизм⁷⁵? Ответ на эти вопросы даст лишь дальнейшее развитие событий. Но уже сейчас есть основания полагать, что текущий кризис в связи с COVID-19 станет предвестником одного из крупнейших переформатирований политического и социально-экономического уклада в современной истории. Ведущую роль в нем будут играть именно цифровые технологии, а в стороне от него, вероятно, не останется практически ни одно государство мира.

⁷⁵ Луддиты - участники стихийных протестов против внедрения машин в ходе промышленной революции в Англии в начале XIX века. С точки зрения луддитов, машины вытесняли из производства людей, что приводило к технологической безработице.

© Счетная палата Российской Федерации, 2020