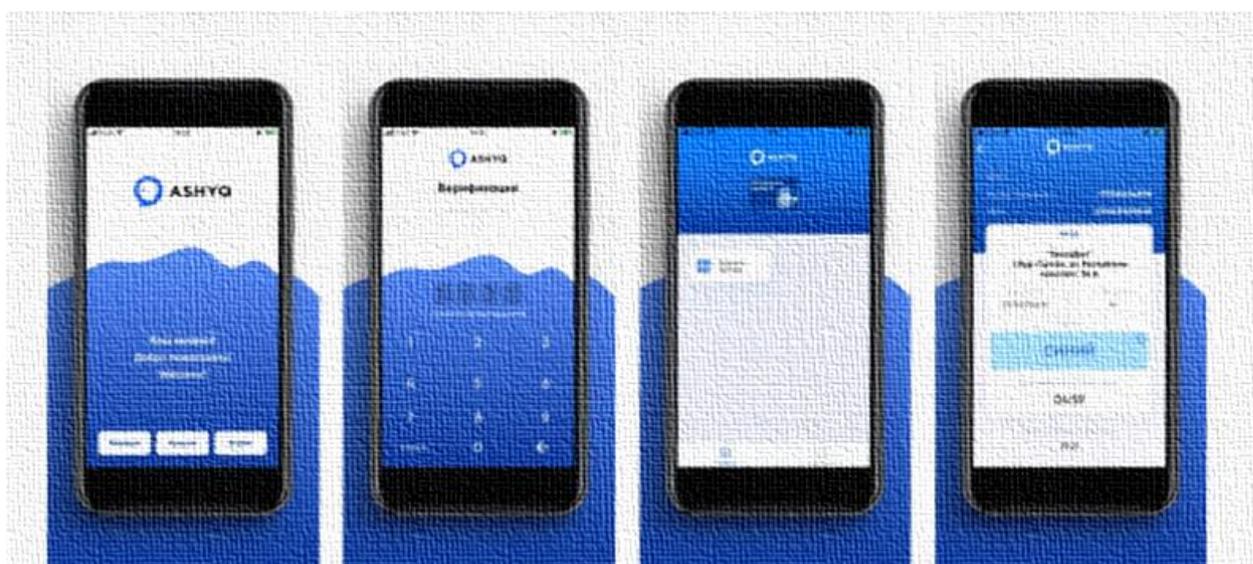


# Ashyq: год спустя, что дальше?



*Анна Гусарова, Серик Джаксылыков*



Проект реализован при финансовой поддержке Фонда Сорос-Казахстан. Точка зрения авторов, отраженная в данном исследовании, может не совпадать с точкой зрения Фонда Сорос-Казахстан. Ответственность за факты, сведения, суждения и выводы, содержащиеся в публикации, несут авторы.

## Содержание

<b>Введение</b>	<b>3</b>
<b>1. Цифровые приложения в борьбе с пандемией COVID-19</b>	<b>4</b>
1.1 Обзор международного опыта: достижения и ошибки	5
1.1.1. Как измерять успех?	9
1.1.2. Законодательная база и правовые трудности	11
1.2 Опыт Казахстана	14
<b>2. Анализ приложения Ashyq: о чем говорят результаты исследования?</b>	<b>20</b>
2.1 Замер общественного мнения казахстанцев	21
2.1.1. Использование системы Ashyq и доверие к ней	21
2.1.2. Персональные данные	29
2.2 Глубинные интервью с экспертами	31
<b>Выводы и рекомендации</b>	<b>35</b>

## Введение

С начала пандемии COVID-19 десятки стран разработали и внедрили цифровые приложения, которые пытаются идентифицировать людей, подвергшихся воздействию коронавируса SARS-CoV-2, и останавливать дальнейшее заражение и распространение коронавируса. Но в демократических странах трудно найти доказательства того, что эти приложения для отслеживания контактов работают, потому что большинство из них собирают ограниченные данные для защиты приватности и конфиденциальности пользователей. Появляются исследования, которые показывают растущее количество доказательств того, что приложения могут действительно помочь предотвратить инфекции и являются ценным инструментом общественного здравоохранения. Однако сами по себе они не смогут взять под контроль пандемию, а должны иметь адекватную политическую поддержку и должным образом интегрироваться в здравоохранение.

С 1 февраля 2021 года по заказу Министерства цифрового развития, инноваций и аэрокосмической промышленности и Министерства здравоохранения стартовал пилотный проект «Ashyq» в Казахстане. Главной целью данного мобильного приложения является минимизация рисков распространения коронавируса, соблюдение санитарных мер и восстановление бизнеса после локдаунов и режима чрезвычайной ситуации из-за волн пандемии. К проекту Ashyq присоединилось многие предприниматели и организации разного масштаба уже по всей стране и благодаря этому они получали возможность работать дольше по времени и иногда в выходные.

Несмотря на многие позитивные моменты, такие как выявление и ограничение доступа контактным и зараженным, связанные с безопасностью людей, есть целый блок вопросов и проблемных точек, которые мы наблюдаем на протяжении уже почти года. К примеру, речь идет о фальсификации статуса (цвета), отсутствие контроля сканирования QR-кода на входе и выходе, отсутствие изменения статуса из-за болезни человека или заражения его/ее несовершеннолетних детей, отсутствие возможностей пользоваться приложением иностранным гражданам, отсутствие смартфонов у некоторых категорий граждан, срок действия статуса (в зависимости от вакцинации, ПЦР и ревакцинации), спекуляция и приобретение фейковых статусов из-за коррупции и многое другое.

Представляется логичным понять, насколько приложение работает эффективно, как решаются вопросы и проблемы, и что будет дальше по мере вакцинации и ревакцинации, избегая манипуляций с технологиями с целью цифровой слежки за гражданами (особенно активистами) и чрезмерного сбора персональных данных в связи с covid-2019 для сохранения их ценности.

В этой связи представляется крайне важным понимать, как казахстанцы относятся к этому приложению, что думают и наблюдают по мере регистрации и пользования, доверяют ли этому приложению или отдают предпочтение другим способам проверки статуса, какие риски беспокоят и пр. И главное, как долго с нами будет оставаться это приложение, постоянно собирающее, обрабатывающее и хранящее наши персональные данные, а также ставя под сомнение приватность и конфиденциальность данных в угоду кажущегося контролю над распространением COVID-19.

## 1. Цифровые приложения в борьбе с пандемией COVID-19

В ответ на COVID-19 многие страны обратились к технологиям цифрового отслеживания контактов (*ТЦОК* или *DCTs*<sup>1</sup>) для борьбы со смертельной пандемией. В широком смысле это приложения, используемые для обнаружения, отслеживания и предоставления разрешения на доступ для изоляции зараженных людей от незараженных<sup>2</sup>. Новые исследования в странах, где были внедрены подобные инструменты, например, в Великобритании и Испании, показывают, что они эффективнее в процессе замедления передачи коронавируса и спасения жизней людей в сравнении с «ручным» отслеживанием контактов.

В сочетании с цифровой инфраструктурой, тестированием, социальным дистанцированием и вакцинами эти технологии обещали революционизировать борьбу с пандемиями и вернуть к нормальной жизни или привычной реальности. Тем не менее, пользователи должны отказаться от некоторой степени приватности и конфиденциальности, поскольку большинство служб отслеживания контактов требуют от них как минимум сообщать данные о своем местоположении. Из этого следует, что общественность опасается позволять правительствам вмешиваться в их частную жизнь.

*«Приложения для изоляции людей от зараженных сторон очень эффективны для замедления передачи COVID-19. Приложения требуют, чтобы правительства собирали данные и определяли ваше местоположение, что приводит к проблемам с приватностью и конфиденциальностью. Существующие нормативные руководства можно эффективно использовать, применяя индивидуальный подход для каждой страны и укрепляя их там, где это необходимо».* Об этом говорили на всемирном экономическом форуме в мае 2021 года<sup>3</sup>, когда стали появляться первые результаты исследований и замеров общественного мнения использования подобных технологий и их реальной пользы в борьбе с распространением пандемии.

Сегодня спустя три года после того, как мир проснулся с коронавирусом, многие из обязательных мер предосторожности, включая ношение масок, ПЦР-тест или антиген-тест, даже вакцинацию, либо частично, либо полностью отменены; однако коронавирус никуда не делся, он продолжает мутировать и жить с человечеством дальше. **А что же произошло с цифровыми технологиями, в частности приложениями, специально разработанными с целью снижения распространения COVID-19?** В одних странах они продолжают активно использоваться, в других - временно приостановлено. **Что дал этот опыт использования цифровых технологий в таком значимом для жизни людей секторе здравоохранения? Какие уроки и ошибки извлекли страны в этом процесс?**

<sup>1</sup> Digital contact tracing technologies, или на русском технологии цифрового отслеживания контактов.

<sup>2</sup> Apps and Covid-19, Privacy International, [Apps and Covid-19 | Privacy International](#).

<sup>3</sup> Digital contact tracing apps help slow COVID-19. Here's how to increase trust, World Economic Forum, May 5, 2021, [Digital contact tracing apps for COVID-19: How to gain trust | World Economic Forum \(weforum.org\)](#).



чилийское Coronapp, датское Smittestop, финское Koronavilkku, GH COVID-19 Tracker из Ганы, итальянское Immuni, нидерландское CoronaMelda, сингапурское TraceTogether и британское приложение NHS. Различные штаты США также создали свои собственные версии, например CA Notify в Калифорнии и COVIDWise в Вирджинии<sup>14</sup>.

Проведенное Amnesty International исследование приложений для борьбы с COVID-19 показало, что приложения, как правило, делятся на три категории<sup>15</sup>:

- ⇒ **Категория 1.** Приложения, которые на самом деле не занимаются цифровым отслеживанием контактов, а позволяют пользователям добровольно записывать и проверять свои симптомы (например, Ливан и Вьетнам).
- ⇒ **Категория 2.** Приложения, которые используют гораздо менее инвазивную децентрализованную модель отслеживания контактов Bluetooth, подобную той, что разработана Google и Apple. В рамках этой модели данные хранятся на телефонах людей, а не в централизованной базе данных. Сюда входят такие страны, как Австрия, Германия, Ирландия и Швейцария.
- ⇒ **Категория 3.** Приложения для отслеживания контактов, которые являются централизованными, то есть они регистрируют данные, полученные через датчик Bluetooth телефона или через GPS (или и то, и другое), и загружают эти данные в централизованную государственную базу данных, а в некоторых случаях являются обязательными.

Таблица 1. Некоторые официальные мобильные приложения по отслеживанию и сдерживанию коронавируса<sup>16</sup>

СТРАНА	МОБИЛЬНОЕ ПРИЛОЖЕНИЕ
Австралия	<b>COVIDSafe app</b> Технология: Bluetooth с низким энергопотреблением Провайдер: Правительство Австралии Использование: добровольное Код: <a href="https://github.com/AU-COVIDSafe">https://github.com/AU-COVIDSafe</a>
Австрия	<b>StoppCorona app</b> Технология: Bluetooth с низким энергопотреблением, Google & Apple API Провайдер: Австрийский красный крест Разработчик: UNIQA & Accenture Austria Использование: добровольное Код: <a href="https://github.com/austrianredcross">https://github.com/austrianredcross</a>
Германия	<b>Corona-warn-app</b> Технология: Bluetooth с низким энергопотреблением, Google & Apple API Провайдер: Немецкое правительство Разработчик: SAP & Deutsche Telekom Использование: добровольное Код: <a href="https://github.com/corona-warn-app">https://github.com/corona-warn-app</a>
Венгрия	<b>Virus radar<sup>17</sup></b> Технология: Bluetooth с низким энергопотреблением Провайдер: Министерство инноваций и технологий Разработчик: Nextsense (оригинальное название приложения 'StopCorona!') Использование: добровольное
Индия	<b>Aarogya Setu app</b> Технология: Bluetooth с низким энергопотреблением и GPS

<sup>14</sup> Covid tracing apps: a comparison of different approaches, [Covid tracing apps: a comparison of different approaches | International Bar Association \(ibanet.org\)](#).

<sup>15</sup> Bahrain, Kuwait and Norway contact tracing apps among most dangerous for privacy, Amnesty International, June 16, 2020, [Bahrain, Kuwait and Norway contact tracing apps among most dangerous for privacy - Amnesty International](#).

<sup>16</sup> Countries with official Contact Tracing Apps, Countries with official Contact Tracing Apps | ndm - 5fb1258.

<sup>17</sup> Приложение 'Virus radar'/'Stop Corona' было запущено в Северной Македонии.

	<p>Провайдер: Индийское правительство          Разработчик: Национальный центр информатики, правительство Индии          Использование: загрузка обязательна для государственных и частных служащих          Код: <a href="https://github.com/nic-delhi/AarogyaSetu_Android">https://github.com/nic-delhi/AarogyaSetu_Android</a></p>
<b>Исландия</b>	<p><b>Rakning C19</b>          Технология: GPS          Провайдер: Правительство Исландии          Использование: добровольное          Код: <a href="https://github.com/aranja/rakning-c19-app">https://github.com/aranja/rakning-c19-app</a></p>
<b>Италия</b>	<p><b>Immuni App</b>          Технология: Bluetooth с низким энергопотреблением, Google &amp; Apple API          Провайдер: Итальянское правительство          Разработчик: Bending Spoons          Использование: добровольное          Код: <a href="https://github.com/immuni-app">https://github.com/immuni-app</a></p>
<b>Латвия</b>	<p><b>Apturi Covid app</b>          Технология: Bluetooth с низким энергопотреблением          Провайдер: Министерство здравоохранения и Центр профилактики и контроля заболеваний          Разработчик: Консорциум латвийских частных компаний          Код: *доступно для адаптации в других странах или сообществах по запросу (<a href="mailto:info@apturicovid.lv">info@apturicovid.lv</a>)</p>
<b>Новая Зеландия</b>	<p><b>NZ Covid Tracer app</b>          Технология: отслеживание местоположения путем сканирования QR-кода          Провайдер: Министерство здравоохранения          Использование: добровольное</p>
<b>Норвегия</b>	<p><b>Smittestopp app</b>          Технология: Bluetooth с низким энергопотреблением и GPS          Провайдер: Правительство Норвегии          Использование: добровольное          Код: <a href="https://github.com/djkaty/no.simula.smittestopp">https://github.com/djkaty/no.simula.smittestopp</a></p>
<b>Соединенное Королевство</b>	<p><b>NHS Covid-19 app<sup>18</sup></b>          Технология: Bluetooth с низким энергопотреблением          Провайдер: NHSX          Разработчик: VMWare Pivotal Labs          Использование: добровольное          Код: <a href="https://github.com/nhsx/">https://github.com/nhsx/</a></p>
<b>Сингапур</b>	<p><b>TraceTogether</b>          Технология: Bluetooth с низким энергопотреблением          Провайдер: Правительство Сингапур          Использование: добровольное          Код: <a href="https://github.com/OpenTrace-community">https://github.com/OpenTrace-community</a> &amp; <a href="https://bluetrace.io">https://bluetrace.io</a></p>
<b>Франция</b>	<p><b>StopCovid app</b>          Технология: Bluetooth с низким энергопотреблением          Провайдер: Французское правительство          Разработчик: Национальный институт исследований в области цифровых наук и технологий (INRIA) и Национальное агентство по обеспечению безопасности информационных систем (ANSSI), Capgemini, Dassault Systèmes, Inserm, Lunabee Studio, Orange, Santé Publique France and Withings          Использование: добровольное          Код: <a href="https://gitlab.inria.fr/stopcovid19">https://gitlab.inria.fr/stopcovid19</a></p>
<b>Чехия</b>	<p><b>eRouska app</b>          Технология: Bluetooth с низким энергопотреблением          Провайдер: Министерство здравоохранения          Разработчик: Consortium of volunteers (Covid19CZ)          Код: <a href="https://github.com/covid19cz/">https://github.com/covid19cz/</a></p>
<b>Швейцария</b>	<p><b>SwissCovid App</b>          Технология: Bluetooth с низким энергопотреблением          Провайдер: Федеральное управление общественного здравоохранения          Разработчик: EPFL и ETH Zürich          Использование: добровольное          Код: <a href="https://github.com/DP-3T/dp3t-app-android-ch">https://github.com/DP-3T/dp3t-app-android-ch</a></p>

<sup>18</sup> Правительство разработало решения на основе API Google и Apple.

Из этой таблицы видно, о каких технологиях идет речь, кто является разработчиком и как эти приложения используются. Несмотря на то, что в большинстве случаев использование выше обозначенных приложений считалось добровольным, по факту в определенных странах в определенный период оно было обязательным, вследствие чего нарушались цифровые права на свободу перемещений и частную жизнь.

Как правило, подобные приложения работают в фоновом режиме на телефоне пользователя и в электронном виде обмениваются индивидуальным кодом ссылки с другими пользователями приложения поблизости — т.н. «цифровое рукопожатие». Затем приложение сохраняет код ссылки вместе с расстоянием между пользователями и продолжительностью их контакта. Если у пользователя положительный результат на COVID-19, данные, собранные из приложения этого пользователя, могут быть использованы для оповещения других пользователей, которые могли контактировать с зараженным, пока они были заразны. В дополнение к автоматизации некоторых аспектов процесса отслеживания контактов использование мобильных приложений позволяет идентифицировать незнакомцев, с которыми инфицированный человек мог контактировать в общественных местах, таких как супермаркеты или в общественном транспорте, но с которыми иначе невозможно было бы связаться.

Хотя каждое из приложений функционально похоже, между моделями существует множество технических и операционных различий. Большинство приложений, в том числе в Австралии, Бельгии, Дании, Финляндии, Италии и Великобритании, используют сигналы Bluetooth для обмена индивидуальными контрольными кодами, чтобы избежать отслеживания местоположения пользователей; тогда как чилийская модель работает с использованием технологии GPS. В **Сингапуре** правительство бесплатно распространило физический токен (TraceTogether Token) среди всех жителей Сингапура, чтобы гарантировать, что люди без смартфона (например, пожилые люди и дети младшего возраста) также имеют доступ к приложению<sup>19</sup>. Как и приложение, токен TraceTogether работает с использованием технологии Bluetooth, при этом контакты сохраняются на устройстве до тех пор, пока пользователь не даст согласие на передачу своих данных органу здравоохранения.<sup>20</sup>

Существуют также определенные различия между методами хранения данных в каждой стране. К примеру, в Австралии, Италии и Сингапуре данные, записанные приложением, хранятся на локальных серверах, а не на конкретном персональном устройстве, как в Нидерландах и Великобритании.

В апреле 2020 года Google и Apple разработали собственный интерфейс прикладного программирования (API) — систему уведомления об экспозиции, встроенную в операционные системы iOS и Android, чтобы обеспечить цифровое отслеживание контактов с помощью фоновых операций Bluetooth. В большинстве стран приложение для отслеживания COVID-19 было построено на базе систем Google и Apple, при этом *Австралия является одной из единственных юрисдикций, разработавших собственную*

---

<sup>19</sup> COVID app triggers overdue debate on privacy in Singapore, [COVID app triggers overdue debate on privacy in Singapore | Technology News | Al Jazeera](#); Contact Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-offs, [2003.11511] [Contact Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-offs \(arxiv.org\)](#).

<sup>20</sup> Covid tracing apps: a comparison of different approaches, [Covid tracing apps: a comparison of different approaches | International Bar Association \(ibanet.org\)](#).

*независимую систему*. Как правило, скачивание приложений не является обязательным, поскольку население принимает приложения на добровольной основе. Однако в Сингапуре есть определенные группы населения и определенные места, где использование приложения (или токена) является обязательным. Рабочие-мигранты должны загрузить приложение или использовать токен в качестве условия получения разрешения на работу. В некоторых местах, таких как рабочие места, школы и рестораны также требуется использование приложения или токена.

Многие правительства отреагировали на проблемы приватности, конфиденциальности и безопасности данных, поднимаемые пользователями и органами по защите данных. К примеру, ганское приложение GN COVID-19 Tracker было пересмотрено и переработано для решения проблемы сообщества, поскольку оно собирало больше пользовательских данных, чем это необходимо для его целей, а также для устранения проблем с целостностью, которые позволяли пользователям вводить данные от имени других лиц<sup>21</sup>.

Точно так же разработчики голландского приложения CoronaMelda ответили на совет Управления по защите данных и прекратили использование правительством анонимных данных о дорожном движении в целях наблюдения за общественным движением во время блокировки<sup>22</sup>. Управление по защите данных выразило обеспокоенность по поводу того, что существует опасность повторной идентификации наборов данных, что может поставить под угрозу конфиденциальность пользователей.

В **Великобритании** от первой версии приложения NHS в итоге отказались из-за проблем с функциональностью, которые не позволяли ему распознавать более 4% находящихся поблизости пользователей iOS и 75% находящихся поблизости пользователей Android. Технические характеристики существенно различаются между текущей и предыдущей версиями, при этом некоторые британские эксперты связывают более точное распознавание находящихся поблизости пользователей с использованием API Google-Apple в текущей версии. Методы хранения также различаются между двумя моделями: записи контактов пользователей теперь хранятся на личном устройстве каждого пользователя, а не на централизованном сервере для решения проблем, связанных с нарушением приватности и конфиденциальности.

### 1.1.1. Как измерять успех?

Пока неясно, как измерить успех в бизнесе приложений COVID-19, и, возможно, никогда не будет понятно. Если количество загрузок или скачиваний по отношению к численности населения, очевидно, является ключевым показателем, оно становится менее важным, если приложение имеет проблемы с функциональностью или считается ненадежным. Многие эксперты по отслеживанию контактов говорят, что даже с хорошо работающим приложением, которое пользуется большой популярностью среди населения, установить точную роль, которую приложение будет играть в сдерживании уровня заражения, непросто. Например, приложения, которые не хранят данные в централизованном месте,

---

<sup>21</sup> Ibid.

<sup>22</sup> Ibid.

могут работать очень хорошо, но нет центрального органа с данными, чтобы точно сказать, сколько людей было успешно предупреждено о риске заражения<sup>23</sup>.

С точки зрения чистого объема загрузок, индийское приложение Aarogya Setu является лидером. В апреле 2020 года оно входило в десятку самых загружаемых приложений в мире, уступая только технологическим гигантам, таким как Zoom, TikTok, Facebook, WhatsApp, Instagram и Messenger. По данным Sensor Tower, консультанта по мобильным приложениям, к середине июля 2020 года Aarogya Setu скачали более 127 миллионов раз. Приложение достигло отметки в 100 миллионов в течение 40 дней после того, как стало доступно<sup>24</sup>. При охвате менее 10% вероятность того, что два человека, скачавшие приложение, вступят в контакт друг с другом, составляет около 1%.

Обзор технологий Массачусетского технологического института публикует «COVID Tracing Tracker» рассматривает различные приложения COVID-19 по всему миру и оценивает приложения по пяти ключевым показателям (добровольность, ограниченность, уничтожение данных, минимизированная прозрачность и технология), присваивая каждому из них звезду<sup>25</sup>. Aarogya Setu получило всего две звезды, при этом рецензенты критиковали приложение за то, что оно не является добровольным для миллионов пользователей, оно не ограничивает использование собираемых данных и собирает больше данных, чем ему нужно.

Некоторые исследования показывают признаки того, что странам с меньшим населением легче добиться коллективной поддержки своих приложений. В Исландии с населением менее 400 000 человек более 40% людей скачали приложение COVID-19 Rakning C-19 в течение месяца после его запуска.

Ирландия с 5 миллионами населения также продемонстрировала первые признаки успеха. Ирландское приложение Covid Tracker было загружено 1,3 миллиона человек в течение восьми дней после его запуска в начале июля. Это сделало его самым быстро загружаемым<sup>26</sup> приложением на душу населения в Европе.

Вместе с тем, как и ожидалось, наименее популярными стали приложения из следующих стран<sup>27</sup>:

- ⇒ **Группа I** – ноль звезд - Алжир, Китай, Иран (больше не используется), Таиланд;
- ⇒ **Группа II** – 1 звезда - Катар, Северная Ирландия, Филиппины, Кувейт, Мексика, Турция и ОАЭ.

К примеру, Турция обязывает людей с положительным результатом теста загрузить приложение и затем поделиться данными с полицией. В Катаре приложение является обязательным для всех граждан и требует доступа к фотографиям. Более того, приложение также имело серьезное нарушение безопасности при запуске. На

<sup>23</sup> COVID-19 tracing apps proving to be a tricky business around the world, [COVID-19 tracing apps proving to be a tricky business around the world | Business | Economy and finance news from a German perspective | DW | 27.07.2020](#).

<sup>24</sup> Ibid.

<sup>25</sup> "A flood of coronavirus apps are tracking us. Now it's time to keep track of them," MIT Technology Review, May 7, 2020, [A flood of coronavirus apps are tracking us. Now it's time to keep track of them. | MIT Technology Review](#).

<sup>26</sup> Компания Nearform, разработчик ирландского приложения, вела переговоры с департаментом здравоохранения штата Пенсильвания, и, как сообщалось, в этом были заинтересованы в этом другие штаты США.

<sup>27</sup> "A flood of coronavirus apps are tracking us. Now it's time to keep track of them," MIT Technology Review, May 7, 2020, [A flood of coronavirus apps are tracking us. Now it's time to keep track of them. | MIT Technology Review](#).

Филиппинах приложение имеет серьезные проблемы с конфиденциальностью, что вызвало письмо с требованием лучшей защиты от крупных организаций. Конкретные политики конфиденциальности и данных в мексиканском приложении в настоящее время довольно расплывчатые. Что касается Китая, то в открытом доступе очень мало информации о том, как работают китайские технологии, однако можно предположить, что цифровая слежка усилилась в период борьбы с пандемией COVID-19. В Бангладеше, например, приложение было создано Shohoz, онлайн-платформой для обмена поездками и продажи билетов и спустя несколько месяцев после выпуска приложение оказалось не очень эффективным<sup>28</sup>.

По данным расследования Amnesty International<sup>29</sup>, бахрейнское приложение BeAware Bahrain, кувейтское Shlonik и норвежское Smittestopp выделяются среди наиболее тревожных инструментов массового наблюдения или цифровой слежки, поскольку они активно отслеживают местоположение пользователей в режиме реального времени или почти в реальном времени, часто загружая данные GPS координат на центральный сервер, что ставит под угрозу конфиденциальность и безопасность сотен тысяч людей. Катарское приложение ENTERAZ может дополнительно активировать отслеживание местоположения в реальном времени для всех пользователей или отдельных лиц (на момент написания оно остается отключенным).

Таблица 2. Технические особенности приложений по борьбе с коронавирусом

<b>Местоположение</b>	Некоторые приложения идентифицируют контакты человека, отслеживая перемещения телефона (например, с помощью GPS или триангуляции от ближайших вышек сотовой связи) и ища другие телефоны, которые находились некоторое время в том же месте.
<b>Bluetooth</b>	Некоторые системы используют «отслеживание близости», при котором телефоны обмениваются зашифрованными токенами с любыми другими ближайшими телефонами через Bluetooth. Легче анонимизировать и, как правило, считается лучшим для приватности и конфиденциальности, чем отслеживание местоположения.
<b>Google/Apple</b>	Многие приложения будут опираться на совместный API, разрабатываемый Apple и Google. Он позволяет телефонам iOS и Android связываться друг с другом через Bluetooth, позволяя разработчикам создавать приложение для отслеживания контактов, которое будет работать для обоих. Позже обе компании планировали встроить это непосредственно в свои операционные системы.
<b>DP-3T</b>	Децентрализованное отслеживание близости с сохранением конфиденциальности. Это протокол с открытым исходным кодом для отслеживания на основе Bluetooth, в котором журналы контактов отдельного телефона хранятся только локально, поэтому ни один центральный орган не может знать, кто был разоблачен.

### 1.1.2. Законодательная база и правовые трудности

*В большинстве стран использование приложений для отслеживания и других технологий обработки данных, связанных с COVID-19, требовало введения в действие специального нормативного акта, разрешающего сбор и использование персональных*

<sup>28</sup> Ibid.

<sup>29</sup> Bahrain, Kuwait and Norway contact tracing apps among most dangerous for privacy, Amnesty International, June 16, 2020, [Bahrain, Kuwait and Norway contact tracing apps among most dangerous for privacy - Amnesty International](#).

*данных. Существовавших ранее законодательных рамок было недостаточно, чтобы наделить правительства такими возможностями по сбору данных.*

Например, парламент **Нидерландов** в консультации с Управлением по защите данных стремился подтвердить законность приложения в соответствии с Общим регламентом по защите данных (GDPR) путем введения новой правовой основы для сбора и обработки персональных данных. Юридические трудности возникли в других юрисдикциях, где правовая основа для сбора и обработки данных правительствами была менее ясной.

В **Болгарии**, например, несмотря на введение специальной законодательной базы для сбора и обработки персональной информации, связанной с COVID-19, использование правительством данных о телекоммуникационном трафике было в итоге запрещено Конституционным судом. Данные о дорожном движении изначально собирались для мониторинга и обеспечения соблюдения обязательных требований изоляции, и полиция и министры правительства могли получить к ним доступ без ордера, однако, если суд позже признал доступ незаконным, данные должны были быть удалены в течение 24 часов. Несмотря на одобрение местного органа по защите данных, Конституционный суд запретил эту практику, посчитав, что объем сбора данных был непропорциональным в сложившихся обстоятельствах.

Точно так же **Дания** изначально использовала агрегированные мобильные данные для отслеживания соблюдения населением требований социального дистанцирования. С тех пор эта практика была прекращена. Однако были высказаны опасения, что сбор и обработка таких данных не имеют законных оснований. Меньшая прозрачность в отношении законности работы приложения в некоторых странах подорвала общественное доверие к приложению. Это привело к меньшему количеству загрузок, что ограничивает эффективность приложения.

В **Чили**, например, есть опасения по поводу отсутствия четкой основы для сбора данных и в некоторых случаях опасения, что данные собираются и обрабатываются в целях, выходящих за рамки согласия, данного пользователями. Приложение также позволяет пользователям вводить конфиденциальные медицинские данные от имени третьих лиц, что может происходить без их ведома или согласия. *Менее одного процента населения Чили загрузили приложение.*

Даже в странах, где приложение сталкивалось с меньшими юридическими сомнениями, было трудно завоевать общественное доверие. *В Австралии менее 30% населения загрузили COVIDSafe, и только 16% и 17% населения Италии и Дании загрузили Immuni и Smittestop* соответственно<sup>30</sup>. В целом низкий уровень использования приложений для отслеживания отражается в других юрисдикциях по всему миру, при этом лишь в нескольких странах, включая Исландию и Ирландию, успешно загрузили более 40% населения.

В конце 2020 года Сингапур достиг 70-процентного уровня внедрения приложения. Двумя основными причинами этого успеха являются распространение токенов<sup>31</sup> TraceTogether для предоставления доступа жителям, не подключенным к цифровым

---

<sup>30</sup> Ibid.

<sup>31</sup> [TraceTogether](#).

технологиям, и активные шаги, предпринятые правительством для содействия вовлечению сообщества и прозрачности. Правительство Сингапура организовало публичный «демонтаж» технологии, чтобы повысить доверие общества к технологии. Негосударственным техническим экспертам и сторонникам открытого исходного кода было предложено «снести» мобильное приложение и технологию токенов, чтобы публично подтвердить<sup>32</sup>, что они будут функционировать только в соответствии с установленным правительством регламентом.

*Различный успех новых технологий обработки данных, связанных с COVID-19, с точки зрения законности, общественного доверия и функциональности подчеркивает необходимость четкой коммуникации для стимулирования участия и доверия пользователей, особенно в отношении технической работы приложения, конфиденциальности, безопасности данных и, что важно, конкретные преимущества для отдельных пользователей, а также новые принципы и органы для имплементации.*

Если общественность сочтет такие органы заслуживающими доверия, то технологии цифрового отслеживания контактов могут завоевать определенный уровень доверия среди пользователей. Тем не менее, учитывая масштаб внедрения и объем данных, те органы утверждения и процессы, которым доверяют в настоящее время, могут оказаться недостаточными для обеспечения приватности и конфиденциальности. А это означает, что могут потребоваться дополнительные обязательные для исполнения руководящие принципы. Одной из областей, представляющих интерес, является обеспечение того, чтобы данные отслеживания контактов могли отслеживать только контактных и никогда не разглашались.

К примеру, Южная Корея и Австралия предлагают удалять данные по истечении определенного периода, и это должно быть реализовано через независимый и заслуживающий доверия наблюдательный орган<sup>33</sup>. В Великобритании Центр этики и инноваций в области данных<sup>34</sup> пытается понять, как общество может пользоваться всеми преимуществами технологиями цифрового отслеживания в рамках этических и социальных ограничений благодаря процессам проверки, основанным на доверии, и построению доверия к технологиям в целом.

---

<sup>32</sup> Kirsten Han, "In Singapore, Covid vs privacy is no contest," [In Singapore, Covid vs privacy is no contest \(lowyinstitute.org\)](https://www.lowyinstitute.org).

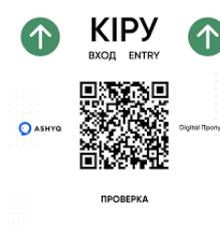
<sup>33</sup> Digital contact tracing apps help slow COVID-19. Here's how to increase trust, World Economic Forum, May 5, 2021, [Digital contact tracing apps for COVID-19: How to gain trust | World Economic Forum \(weforum.org\)](https://www.weforum.org).

<sup>34</sup> Centre for Data Ethics and Innovation, [Centre for Data Ethics and Innovation - GOV.UK \(www.gov.uk\)](https://www.gov.uk).

## 1.2 Опыт Казахстана

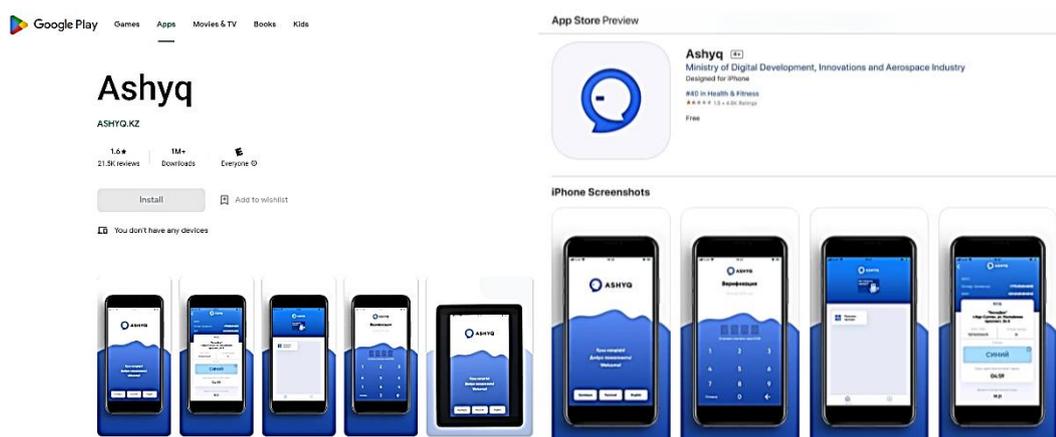
В Казахстане в тестовом режиме мобильное приложение Ashyq<sup>35</sup> было запущено 17 января 2021 года. Впоследствии уже 26 февраля 2021 года принято постановление Главного государственного санитарного врача РК № 7 «О проведении пилота по внедрению мобильного приложения «Ashyq» на объектах предпринимательства в городах Нур-Султан, Алматы и Караганда»<sup>36</sup>. С 5 мая 2021 года доступ в общественные заведения страны стал возможен только при условии сканирования QR-кода через приложение Ashyq<sup>37</sup>. Мобильное приложение Ashyq разработано отечественной IT-компанией TOO Digital Innovation and Transformation с очень интересной историей<sup>38</sup> и было передано на безвозмездной основе Министерству цифрового развития, инноваций и аэрокосмической промышленности.

Согласно portalу eGov<sup>39</sup>, «мобильное приложение Ashyq позволяет за счет использования QR-кода и интеграции с общей базой Министерства здравоохранения определить статус посетителя: является ли он на данный момент носителем вируса или нет, а для бизнеса дает возможность продолжать свою деятельность в период карантинных мер, а также позволяет минимизировать риски распространения COVID-19 и сокращает количество контактов, приводящих к заражению».



Приложение Ashyq доступно в виде бесплатных мобильных приложений на платформах iOS и Android, а также имеет веб-версию и являлось обязательным в использовании. Кроме того, этот сервис интегрирован в другие социально-значимые мобильные приложения, такие как eGov Mobile и приложения банков (Kaspi, Halyk, Sberbank).

*Print Screen со страниц Google Play и App Store*



<sup>35</sup> [ASHYQ](#)

<sup>36</sup> Постановление Главного государственного санитарного врача Республики Казахстан от 26 февраля 2021 года № 7 «О проведении пилота по внедрению мобильного приложения «Ashyq» на объектах предпринимательства в городах Нур-Султан, Алматы, и Караганда», [Постановление Главного государственного санитарного врача Республики Казахстан от 26 февраля 2021 года № 7 «О проведении пилота по внедрению мобильного приложения «Ashyq» на объектах предпринимательства в городах Нур-Султан, Алматы, и Караганда» \(утратило силу\) \(zakon.kz\)](#).

<sup>37</sup> В основном казахстанцы «синие». Приложение Ashyq спасет бизнес от банкротства, но это не точно, [В основном казахстанцы «синие». Приложение Ashyq спасет бизнес от банкротства, но это не точно \(azattyq.org\)](#).

<sup>38</sup> Подарок на миллион: Кто стоит за приложением Ashyq? <https://www.caravan.kz/gazeta/podarok-na-million-kto-stoit-za-prilozheniem-ashyq-734168/>.

<sup>39</sup> [Приложение Ashyq | Электронное правительство Республики Казахстан \(egov.kz\)](#).

По информации, доступной на платформе Google Play, приложение Ashyq скачали более 1 миллиона человек, в то время как на платформе iOS это приложение занимает 40 место в рейтинге приложений по здоровью и фитнесу. В двух системах оценка данного приложения очень низкая, чуть выше 1,5 балла из 5, при том, что оценивали Ashyq 24,500 человек на Android и 4,800 человек на iOS<sup>40</sup>. Большинство негативных комментариев и отзывов связано с цифровой слежкой, нарушением прав человека, критикой власти и принимаемых решений, а также техническими ошибками и проблемами.

Таблица 3. Цитаты\* отзывов по приложению Ashyq с Android и iOS<sup>41</sup>

«Лучше назовите это приложение «Жабық». Полностью описывает текущее состояние приложения. Потратил некоторое время, пытаюсь получить SMS, но произошло несколько ошибок. Мой номер и личные данные уже есть в БМГ, а в мобильном приложении eGov у меня таких проблем нет. Итак, в чем проблема разработать простое приложение, которое просто вызывает внешние государственные службы?»

«Стыд. Это приложение следует запретить, так как оно собирает личные данные о том, куда люди ходят, и маркирует людей по их собственным критериям, которые недостаточно объяснены в приложении. Кроме того, они заставляют бизнес настраивать его для сбора личных данных, не позволяя некоторым предприятиям работать, если они не заставляют своих клиентов использовать это приложение для обмена личными данными с разработчиками».

«Это приложение представляет собой паноптикум для казахстанцев. Постоянная слежка и нарушение прав человека. Местные предприятия должны установить это устройство, а граждане должны загрузить это приложение, чтобы посещать общественные места, такие как фитнес-центры, торговые центры и другие места. Оправдание правительства для запуска этого приложения связано с контролем людей, которые контактировали с COVID-19, но на самом деле за ними наблюдает «Большой брат». Надеюсь, глобальные организации, защищающие права человека, обратят внимание на эту вопиющую акцию!».

«Нарушение прав и несоответствующий уровень разработки приложения. Во-первых, как уже было сказано, приложение нарушает право казахстанцев на неприкосновенность личной информации. Зачем мне делиться своим удостоверением личности с третьей стороной? Во-вторых, если вы делаете приложение обязательным для использования, убедитесь, что оно работает идеально. Проблем со скачиванием быть НЕ должно и ВООБЩЕ НЕТ зависаний. Особенно, когда человек вводит личную информацию, которая, будучи честной, НЕ МОЖЕТ быть передана кому-либо. Так что, по сути, любой человек может подать в суд на разработчиков приложения».

«Оно не работает должным образом. Оно не обновляется автоматически. Нужно позвонить в службу поддержки и попросить их обновить статус. Однако связаться со службой поддержки — еще одна проблема. Они сказали, что это связано с общей базой, к сожалению, это не так. Таким образом, оно не работает должным образом. Очередная трата денег от государства».

«Плохо, очень плохо. Худшее приложение, которое я когда-либо видел. Отставание, отображение неправильного статуса, иногда автоматический выход из системы. Кажется, оно работает так, как хочет, игнорируя пожелания и права клиентов. Уважаемая команда Apple, удалите приложение как можно скорее, приложение не соответствует вашему уровню, не заслуживает скачивания, смотрите все отзывы и принимайте правильное решение. Заранее спасибо!»

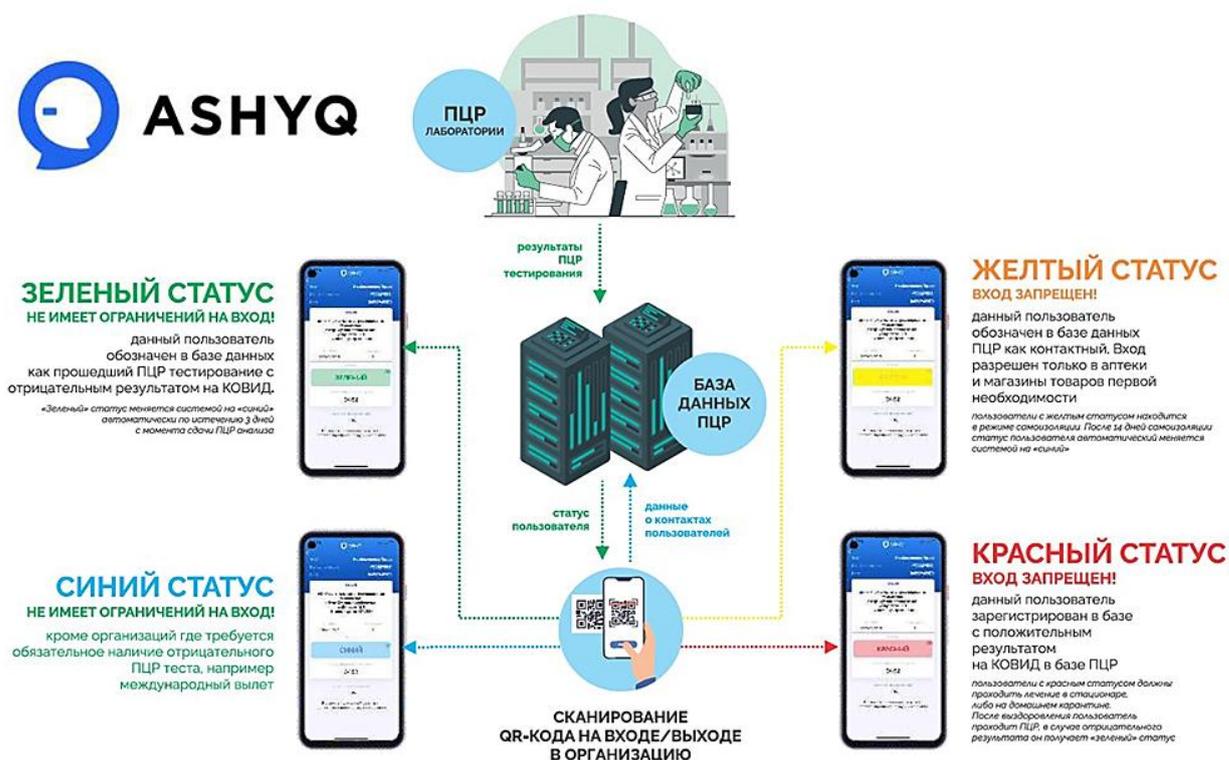
«Бесполезный софт, никакой помощи людям. Уважаемые дизайнеры и разработчики Ashyq, не могли бы вы решить простую и основную вашу задачу, как обновить мой статус после полной вакцинации Pfizer? Я отправил вашей поддержке и помощнику по телефону справку о прививках, но уже 3 недели не могу обновить свой статус на зеленый. Я уже подозреваю вашу программу как бесполезную, не для людей».

\* Реальное отношение казахстанцев к приложению Ashyq см. в Разделе 2.

<sup>40</sup> [Ashyq on the App Store \(apple.com\)](#), [Ashyq - Apps on Google Play](#).

<sup>41</sup> Пунктуация и написание сохранены.

## Что такое Ashyq и как им пользоваться?<sup>42</sup>



## 1. КАК ИСКЛЮЧИТЬ ВХОД БОЛЬНЫМ И КОНТАКТНЫМ?

3



- Пользователь устанавливает на свой смартфон приложение «ASHYQ»
- Проходит процесс регистрации в приложении. Заполняет свои данные (ИИН, номер телефона, адрес проживания)
- При входе в заведение с помощью приложения сканирует QR-код заведения
- Демонстрирует сотруднику заведения свой статус:



При отсутствии смартфона у посетителей в приложении имеется функция для сотрудников, которые смогут при помощи ввода ИИН проверить статус посетителя с его согласия

В начале было необходимо сканировать QR-код при входе и выходе из общественного места (с момента старта проекта условие было обязательным), однако, согласно постановлению главного санитарного врача от 13 апреля 2021 года сканировать QR-код при выходе было больше не надо<sup>43</sup>.

<sup>42</sup> Приложение «Ashyq», [Приложение "Ashyq" \(www.gov.kz\)](http://www.gov.kz).

<sup>43</sup> [Проектный офис ответил на вопросы проекта Ashyq | Inbusiness.kz](#)

Ст. 273 Кодекса РК «О здоровье народа и системе здравоохранения»<sup>44</sup> допускает «предоставление сведений без согласия лица при угрозе распространения заболеваний, представляющих опасность для окружающих», поэтому использование приложения Ashyq не нарушало закон о защите персональных данных. Тем не менее, многие эксперты, юристы, правозащитники и представители общественности и бизнес-среды негативно отнеслись к идее внедрения приложения, объясняя это «незаконным<sup>45</sup>, небезопасным и безосновательным»<sup>46</sup>.

По состоянию на 7 мая 2021 года, т. е. за три месяца работы приложения с момента его внедрения, 817,000 казахстанцев использовали приложение Ashyq<sup>47</sup>. Больше информации о том, сколько казахстанцев используют приложение и какое количество субъектов МСБ внедрили Ashyq отсутствует в открытом доступе, в результате чего трудно оценивать эффективность приложения с точки зрения предотвращения распространения коронавируса. Согласно данным НПП Атамекен, в среднем 3 тысячи граждан в сутки пользовались этим сервисом по состоянию на май 2021 года, при этом в день удаленно выявлялись 80–130 граждан с «красным» статусом<sup>48</sup>. По данным от 6 сентября 2021 года, в системе Ashyq насчитывалось более 4 млн пользователей. При этом приложение позволяло выявлять «красных» и «желтых» нарушителей в Атырау, Шымкенте, Актобе и других городах<sup>49</sup>.

На основе ограниченных данных, доступных в открытом доступе, «за время пилотного апробирования мобильного приложения Ashyq было предотвращено заражение минимум 2,000 граждан»<sup>50</sup>. Более того, были выявлены и не допущены в общественные места более 100,000 человек с положительным статусом ПЦР или контактных<sup>51</sup>. Исходя из этих данных возникает логичный вопрос, *насколько соразмерным и необходимым было внедрение мобильного приложения Ashyq, чтобы противостоять распространению коронавируса в Казахстане и стабилизировать эпидемиологическую ситуацию особенно в моменты «наихудшего сценария»?*

<sup>44</sup> Ст. 273 Кодекса РК О здоровье народа и системе здравоохранения Тайна медицинского работника от 7 июля 2020 года № 360-VI ЗРК Кодекс Республики Казахстан О здоровье народа и системе здравоохранения Статья 273 Комментарий - Законодательство Республики Казахстан 2021 год (kodeksy-kz.com)

<sup>45</sup> Это приложение незаконно - адвокат о введении "антиковидных" QR-кодов в Казахстане - Новости | Караван (caravan.kz).

<sup>46</sup> Нет свободы и биологическая дискриминация: что думают эксперты о приложении Ashyq - Liter.kz.

<sup>47</sup> Приложение Ashyq используют 817 тысяч казахстанцев | Национальная палата предпринимателей Республики Казахстан «Атамекен» (atameken.kz).

<sup>48</sup> ASHYQ | Национальная палата предпринимателей Республики Казахстан «Атамекен» (atameken.kz).

<sup>49</sup> «Атамекен»: 77 тыс. казахстанцев нарушили карантинные ограничения | Национальная палата предпринимателей Республики Казахстан «Атамекен» (atameken.kz)

<sup>50</sup> Как работает приложение Ashyq - Капитал (kapital.kz)

<sup>51</sup> Разработчики Ashyq выиграли суд против предпринимателя (baigenews.kz).

Что касается бизнеса, то ситуация получилась неоднозначная. Некоторые малые предприятия, получившие QR-код для Ashyq, говорили, что потребители недовольны приложением, но соглашались, что это единственный способ удержаться на плаву во время эпидемии коронавирусной инфекции и не стать банкротом. К примеру, директор по продажам фитнес-клуба Fidelity Сергей Безбородов сказал, что «установление приложения Ashyq в начале

*«Многие люди отказались посещать спортзал после того, как ввели приложение Ashyq. Нам поставили ультиматум: либо вы стоите закрытые, либо работаете с Ashyq. То есть выбора не было. Конечно, лучше уж как-то работать, чем вообще не работать. Бизнесу всё равно, работать с Ashyq или без него. Но не всё равно клиенту. Однозначно многие люди не захотели приходить из-за Ashyq». Директор сети тренажерных залов «Банзай» Хаким Курмангалиев*

марта позволило его компании продолжать работу»<sup>52</sup>.

Разработчики приложения Ashyq говорят, что «приложение объединено с базой данных лиц, сдававших ПЦР-тесты, и людей, контактировавших с больными (сделано санврачами) ... Эта информация в приложении обновляется в соответствии с постановлением главного санитарного врача. Человек, у которого выявили коронавирус в результате ПЦР-теста, отмечается в приложении красным цветом и его статус не меняется в течение 14 дней. Желтым

цветом обозначается статус контактировавших с инфицированными больными, и он также сохраняется в течение 14 дней»<sup>53</sup>. Но не все так гладко происходило на деле при регистрации и входе: многие жаловались на отсутствие обновлений или неверный статус, отсутствие результатов ПЦР-теста или паспорта вакцинации, или же некорректности баз данных, включая отсутствие изменений по членам семьи больного или контактного лица. Об этом говорила депутат мажилиса Снежанна Имашева, которая засомневалась в безопасности приложения Ashyq:

*«... приложение собирает номера телефонов и ИИН, однако, что будет в дальнейшем с персональными данными казахстанцев – неизвестно. Итоги двухмесячного пилота Ashyq пользователи оценивают не так радужно, как отчитывало министерство, а само приложение не ругал разве что ленивый. Пользователи оставили около 3 тысяч критических отзывов, запросов и жалоб на его работу. Вызывает беспокойство и то, что приложение собирает персональные данные - номер телефона и ИИН - и неизвестно, в каких еще целях они могут быть использованы в дальнейшем.*

<sup>52</sup> [В основном казахстанцы «синие». Приложение Ashyq спасет бизнес от банкротства, но это не точно \(azattyq.org\).](https://azattyq.org)

<sup>53</sup> Ibid.

*Например, что будет с собранными данными пользователей, после того как отпадет необходимость использовать приложение».<sup>54</sup>*

---

28 апреля 2021 года (два месяца с момента внедрения Ashyq) депутат мажилиса Снежанна Имашева также добавила, что приложение еще не прошло проверку на информационную безопасность. Получается, что *данный цифровой инструмент был внедрен без предварительной проверки или испытаний на соответствие требованиям информационной безопасности и с целью оценки качества*. Согласно ст.49-50 закона Об информатизации<sup>55</sup>, «испытания на соответствие требованиям информационной безопасности проводятся в обязательном порядке или по инициативе собственника или владельца», а также «на этапе создания, внедрения и эксплуатации информационных систем по инициативе собственника или владельца информационных систем может быть проведен аудит информационных систем». Однако *детали подобных проверок при их проведении остаются вне публичного поля и не доступны широкой общественности*, а на сайте НПП Атамекен доступна только ограниченная информация.

*Ответ НПП Атамекен на вопросы по использованию Ashyq<sup>56</sup>*

---

**3. Нарушает ли вход в заведения через Ashyq конституционные права граждан на свободное передвижение?**

*Конституционные права граждан не нарушаются, т. к. Ashyq внедряется субъектами предпринимательства добровольно. Владелец объекта – участник проекта Ashyq – принимает на себя обязательство проверки статусов посетителей. На сегодня при попытке войти на объекты выявлено 1236 граждан с «красным» статусом и 541 человек – с «желтым». Проверка статусов посетителей, в первую очередь, даёт преимущества для самих посетителей. Поскольку, попадая на объект, работающий по Ashyq, риски быть контактным с COVID-положительным человеком минимизируются.*

*Также предприниматели-участники проекта получают преференции по графику работы по сравнению с другими субъектами бизнеса, так как приложение позволяет выявлять инфицированных граждан.*

**6. Как обеспечивается безопасность персональных данных (номера телефонов и ИИН)?**

*Приложение Ashyq находится в защищенном контуре на серверах АО «Национальные информационные технологии», которое является оператором информационно-коммуникационной инфраструктуры «электронного правительства». Следовательно требования к Информационной безопасности повышенные.*

**7. Есть ли у приложения возможность отслеживать местонахождение граждан?**

---

<sup>54</sup> [Депутат раскритиковала работу приложения Ashyq - Капитал \(kapital.kz\).](#)

<sup>55</sup> [Закон Республики Казахстан от 24 ноября 2015 года № 418-V «Об информатизации» \(с изменениями и дополнениями по состоянию на 14.07.2022 г.\) \(zakon.kz\)](#)

<sup>56</sup> [Приложение Ashyq используют 817 тысяч казахстанцев | Национальная палата предпринимателей Республики Казахстан «Атамекен» \(atameken.kz\).](#)

*Мобильное приложение Ashyq не имеет функции отслеживания местонахождения граждан. В настройках телефона каждый пользователь может посмотреть, к чему приложение запрашивает доступ.*

---

Наконец, использование приложения Ashyq сопряжено с некоторыми законодательными обязательствами. В случае заболевания человек должен находиться дома в изоляции 14 дней или с момента контакта с вероятным или подтвержденным случаем коронавируса.<sup>57</sup> В случае нарушения после четырех месяцев работы Ashyq вводился административный штраф в размере 30 МРП<sup>58</sup>.

Данные Комитета санитарно-эпидемиологического контроля при Министерстве здравоохранения РК говорят о том, что наряду с активным использованием приложения Ashyq одновременно начались проверки субъектов бизнеса и обычных граждан на предмет выявления нарушений режима карантина. По разным данным, численность нарушителей в разных регионах разная: были созданы специальные мониторинговые группы, которые выявляли нарушителей. **«За половину 2021 года было проведено 94,788 рейдов, проверено 585,343 объекта, более 16,000 объектов бизнеса работали с нарушением карантинных требований. В лидерах нарушителей оказались организации в Восточно-Казахстанской, Туркестанской и Алматинской областях, в Алматы и Шымкенте».**<sup>59</sup>

---

*С января по май 2021 года казахстанцы заплатили штрафы за нарушение карантинных ограничений на сумму более 1,2 млрд тенге. В суде были начаты 300 дел, 76 объектов бизнеса приостановили свою деятельность. За нарушение правил карантина были оштрафованы 9,100 предприятий МСБ и 6,800 физических лиц<sup>60</sup>. Для сравнения в 2020 году казахстанцы заплатили 12,6 млрд тенге в виде налога на имущество и порядка 50 млрд тенге в виде налога на транспорт<sup>61</sup>.*

---

Год спустя с момента запуска приложения Ashyq 11 марта 2022 года было принято решение его отменить, впрочем, как и ношение масок во всех «зеленых» и «желтых» зонах риска распространения коронавируса.<sup>62</sup> Логично предположить, что по итогам пилотного проекта было бы правильно провести исследование и понять, насколько правильным, ресурсозатратным, соразмерным и необходимым было принятие подобного решения для прекращения или снижения распространения коронавируса в стране; выявить все ошибки, признать их и провести работу на ошибками, чтобы быть готовыми к новым вызовами в системе здравоохранения в первую очередь и менеджмента и управления на местах.

---

<sup>57</sup> [Домашний карантин длится 14 дней с момента последнего близкого контакта с вероятным или подтвержденным случаем COVID-19 \(www.gov.kz\).](http://www.gov.kz)

<sup>58</sup> Ст. 425 КОАП РК, [Об административных правонарушениях - ИПС "Әділет" \(zan.kz\).](http://zan.kz)

<sup>59</sup> [За нарушение карантина казахстанцы заплатили более 1,2 млрд тенге - 03.06.2021 - Kursiv Media Казахстан.](http://kursivmedia.kz)

<sup>60</sup> [Как соблюдаются санитарные нормы в регионах Казахстана - 03.06.2021 | Strategy2050.kz - обзорно-аналитический портал Казахстана.](http://strategy2050.kz)

<sup>61</sup> [Невидимые миру деньги: сколько налогов незаметно платят казахстанцы каждый день. Инфографика \(ism.kz\).](http://ism.kz)

<sup>62</sup> [В Казахстане отменили ASHYQ и ношение масок | OTYRAR.](http://otyrary.kz)

## 2. Анализ приложения Ashyq: о чем говорят результаты исследования?

Данное исследование является продолжением двух исследований, проведенных в 2019<sup>63</sup> и 2020<sup>64</sup> годах. Предметом этих исследований является отношение казахстанцев к безопасности персональных данных, их осведомленность в вопросах защиты персональных данных, а также знание своих прав в этой сфере. В данном исследовании этот предмет рассматривается через призму опыта использования системы Ashyq и доверия к ней.

В исследовании используются первичные данные, собранные методом телефонного опроса. Выборка репрезентативна для взрослого населения Казахстана, в опросе участвовали резиденты страны в возрасте 18 лет и старше. Всего было опрошено 1317 человек.

Проведенный опрос не выявил признаков широко распространенного неприятия или недоверия в отношении системы Ashyq и его мобильного приложения. Подавляющее большинство казахстанцев (77%) пользовалось этой системой в тех местах, где это было необходимо. Численность людей, когда-либо пользовавшихся системой Ashyq, определялась географическим охватом этой системы и назначением мест, в которых она применялась. Те, кто не пользовался системой Ashyq, по большей части представлены людьми старшего поколения и жителями сел и малых городов. Первые в силу своего возраста и образа жизни обходились без посещения общественных мест, доступ к которым требовал проверки статуса по коронавирусу, а в небольших населенных пунктах такие места встречались намного реже.

Доля людей, которые не пользовались системой Ashyq по причине недоверия к ней, незначительна (меньше пределов погрешности данных). Лишь небольшая доля (17%) опрошенных выразила недоверие системе и мобильному приложению Ashyq. При этом значительная их часть не доверяет этой системе с точки зрения ее эффективности в качестве меры против пандемии.

В то же время, по меньшей мере **каждый третий (36%) опрошенный считает или допускает большую вероятность того, что это приложение было разработано таким образом, чтобы отслеживать персональные данные граждан.**

**43% опрошенных считают, что имели ли место случаи подделки эпидемиологического статуса или доступа в общественные места в обход системы Ashyq, в том числе 13% считают, что такие случаи были широко распространены.**

Что касается защиты персональных данных, то **каждый четвертый (27%) опрошенный сильно обеспокоен проблемой безопасности персональных данных, которые предоставляет онлайн. 46% казахстанцев не знают (25%) или имеют минимальные,**

<sup>63</sup> Анна Гусарова, Серик Джаксылыков, Защита персональных данных в Казахстане: статус, риски и возможности, 2020, <https://www.soros.kz/ru/protection-of-personal-data-in-kazakhstan-status-risks-and-opportunities/>

<sup>64</sup> Anna Gussarova, Serik Zhaksylykov, Data Protection in Kazakhstan 2.0 COVID-19 Digital Footprint, March 2021, [Data Protection in Kazakhstan 2.0 COVID-19 Digital Footprint \(caiss.expert\)](https://www.soros.kz/ru/data-protection-in-kazakhstan-2.0-covid-19-digital-footprint-caiss-expert/).

очень ограниченные знания (21%) о защите персональной информации, предоставляемой онлайн. Каждый второй (55%) житель страны не знает (29%) или знает очень мало (26%) о своих правах в сфере защиты персональной информации, предоставляемой онлайн.

## 2.1 Замер общественного мнения казахстанцев

### 2.1.1. Использование системы Ashyq и доверие к ней

77% опрошенных проверяли свой статус по коронавирусу в системе Ashyq, чтобы войти в общественные места во время карантинных ограничений против COVID-19. Полученные данные подтвердили предположение о том, что доля тех, кто пользовался этой системой, была заметно меньше среди жителей сельской местности, здесь их доля составила 67%. Если сравнить ответы жителей разных типов поселений, то можно наблюдать постепенное снижение доли пользовавшихся системой Ashyq от самых крупных городов страны (города республиканского значения) к селам (см. *Диаграмму 2*): города республиканского значения – 87%, областные центры – 82%, города областного или районного значения – 82%, села – 67%.

Диаграмма 1. Вопрос: «Приходилось ли вам проверять свой статус по коронавирусу в системе Ashyq, чтобы входить в общественные места во время действия карантинных ограничений против COVID-19?» Все респонденты, N = 1317

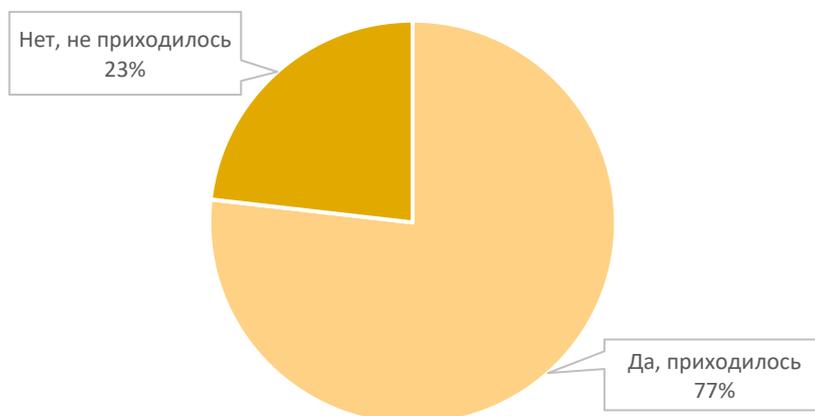


Диаграмма 2. Вопрос: «Приходилось ли вам проверять свой статус по коронавирусу в системе Ashyq, чтобы входить в общественные места во время действия карантинных ограничений против COVID-19?», распределение ответов в возрастных группах и типах поселений. Все респонденты, N = 1317



Объяснение наблюдаемой градации по типу поселения нужно искать не в разнице взглядов городских и сельских жителей, а прежде всего в разнице социальной инфраструктуры крупных и малых городов и сел. Дело в том, что в сельской местности число общественных мест, для доступа к которым было необходимо подтверждать статус по коронавирусу, было значительно меньше. Ниже приведена диаграмма распределения ответов сельских жителей (см. *Диаграмму 3*), которые имеют опыт проверки статуса в системе Ashyq, и на ней видно, что из их числа только 40% делали это в селе.

Диаграмма 3. Вопрос: «В каких населенных пунктах страны вам приходилось проверять свой статус по коронавирусу в системе Ashyq?». Сельские жители, которым приходилось подтверждать свой статус в системе Ashyq, N = 352.



Еще одним фактором, который связан с использованием системы Ashyq, очевидно, является возраст. Согласно полученным данным (см. *Диаграмму 2*), наименьшая доля тех, кто пользовался Ashyq, наблюдается среди самых взрослых респондентов: в возрасте от 51 до 63 лет – 61%, в возрасте от 64 лет и старше – только 55%. С одной стороны, это может быть связано с тем, что многие общественные места, на входе в которые действовала система Ashyq, были представлены торгово-развлекательными центрами, кинотеатрами, магазинами, ориентированными преимущественно на молодую аудиторию, то есть люди старшего поколения просто реже оказывались в тех местах, где было необходимо проверять статус посредством Ashyq. С другой стороны, это также связано с тем, что

использование мобильного приложения для проверки статуса могло вызывать затруднения для людей старшего поколения. Но главной причиной, как будет показано ниже, является то, что люди старшего поколения вообще редко выходят из дома, редко посещают общественные места без большой необходимости.

Тем респондентам, которые не пользовались системой Ashyq, был задан вопрос о причинах отсутствия такого опыта. Наиболее часто (29%) респонденты говорили, что просто «никуда не ходили» (или, например, «были за границей»). 21% респондентов сказали, что обходились теми местами, в которых не требовалось обращение к системе Ashyq (см. Диаграмму 4).

Только 16% ответивших на этот вопрос, сказали, что сознательно избегали таких мест, где требовалась проверка статуса по коронавирусу. Этим респондентам задавался вопрос о причинах такой позиции, на что 40% из них сказали, что просто никуда не ходили (смотрите Диаграмму 5). Примерно каждый четвертый (27%) из них выбрал варианта ответа «не знал, как это работает, и что нужно делать». Только 7% сказали выбрали вариант ответа «я не доверяю системе Ashyq, и еще 10% - вариант «я не хочу устанавливать дополнительные мобильные приложения».

Диаграмма 4. Вопрос: «Почему вы не пользовались системой Ashyq?» Респонденты, которые не пользовались системой Ashyq, N = 305.

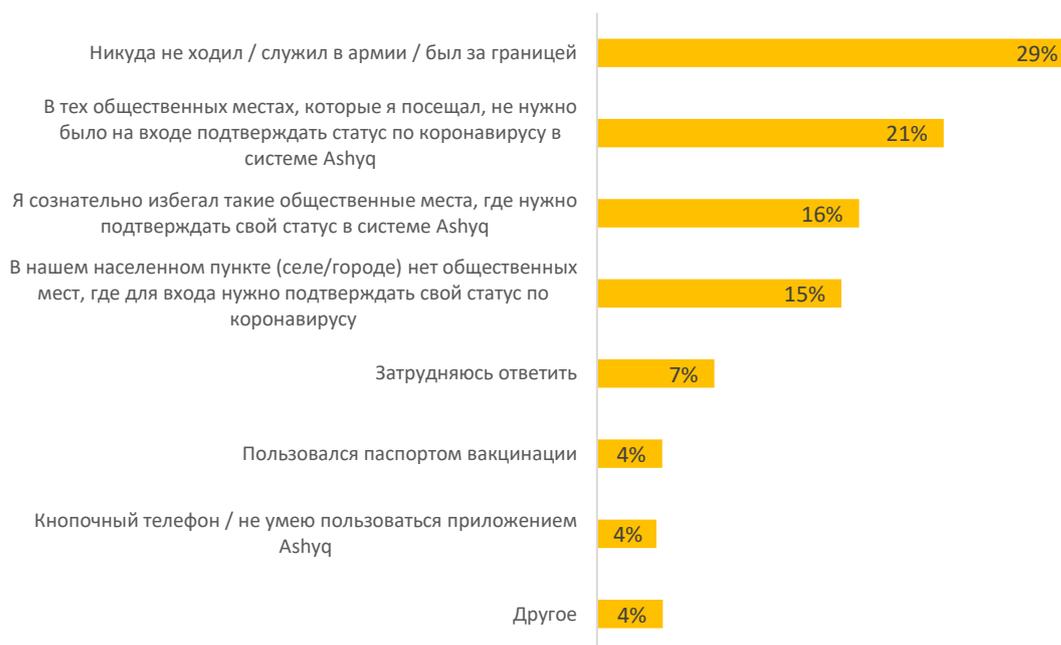


Диаграмма 5. Вопрос: «Почему вы избегали таких общественных мест, где было необходимо подтвердить свой статус в системе Ashyq?» Респонденты, которые ответили, что сознательно избегали мест, в которых требовалось подтверждение карантинного статуса, N = 49.



Показателем уровня доверия мобильному приложению Ashyq может служить выбор людей – каким приложением пользовались для проверки статуса по коронавирусу. Приложением Ashyq пользовалось 40% респондентов, ответивших на этот вопрос. Это второе место в условном рейтинге после мобильного приложения «Каспи»/Kaspi, которым пользовалось 57% респондентов. Все остальные способы обращения к системе Ashyq сильно отстают, к примеру, оказавшееся на третьем месте мобильное приложение «Халык банка»/Haluk отметило лишь с 8% респондентов.

Диаграмма 6. Вопрос: «Каким способом вы подтверждали свой статус по коронавирусу в системе Ashyq?». Респонденты, которым приходилось подтверждать свой статус в системе Ashyq, N = 1012.



Всем респондентам, принявшим участие в опросе, был задан вопрос о доверии системе/приложению Ashyq. Согласно полученным данным, подавляющее большинство (70%) опрошенных доверяют Ashyq, а доля тех, кто выразил свое недоверие, составила 17% (см. *Диаграмму 7*). Следует отметить, что такое распределение ответов наблюдается во всех типах поселений – от крупнейших городов до сел (см. *Диаграмму 8*).

Диаграмма 7. Вопрос: «Доверяете ли вы системе/приложению Ashyq?». Все респонденты, N = 1313.

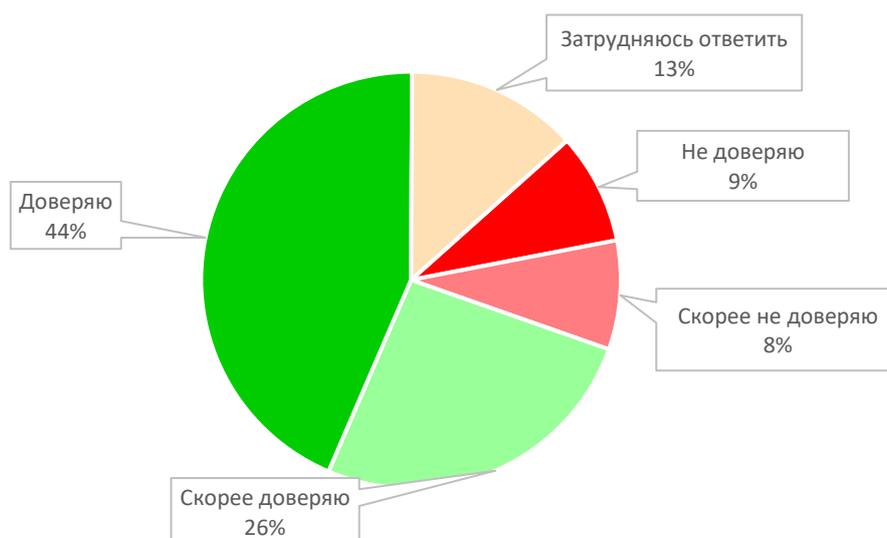
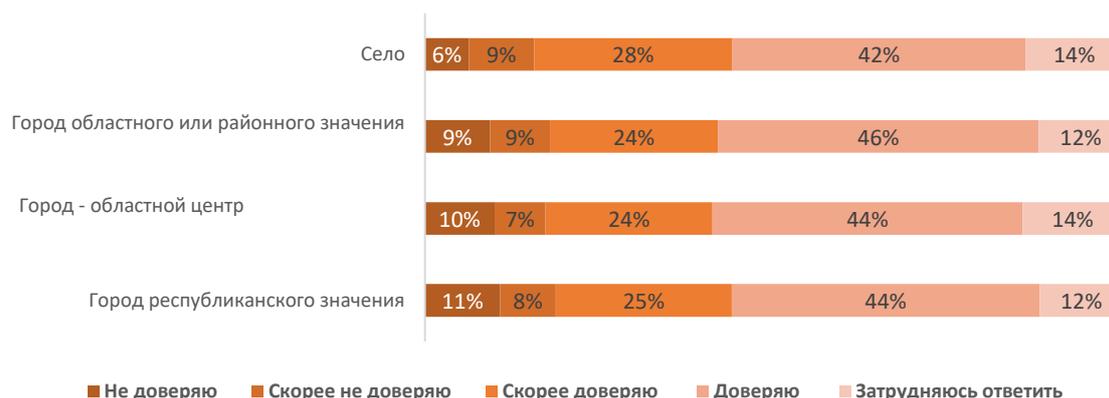


Диаграмма 8. Вопрос: «Доверяете ли вы системе/приложению Ashyq?», распределение ответов в разных типах поселений. Все респонденты, N = 1313.



Чтобы понять, что стоит за отсутствием доверия системе Ashyq, всем респондентам, выразившим свое недоверие, был задан соответствующий вопрос. Как оказалось, чаще всего недоверие приложению объясняется тем, что его не воспринимают как эффективный инструмент борьбы с пандемией: четверо из десяти (42%) опрошенных «не верят, что эта система может помочь в борьбе с пандемией» (см. Диаграмму 9).

Далее, с заметным отставанием, следуют другие три причины, одна из которых связана непосредственно с безопасностью персональных данных: «я боюсь, что мои персональные данные могут быть похищены» - 20%, «я боюсь хакерского взлома через это мобильное приложение» - 20%, «я не доверяю мобильным приложениям, разработанным в нашей стране» - 19%.

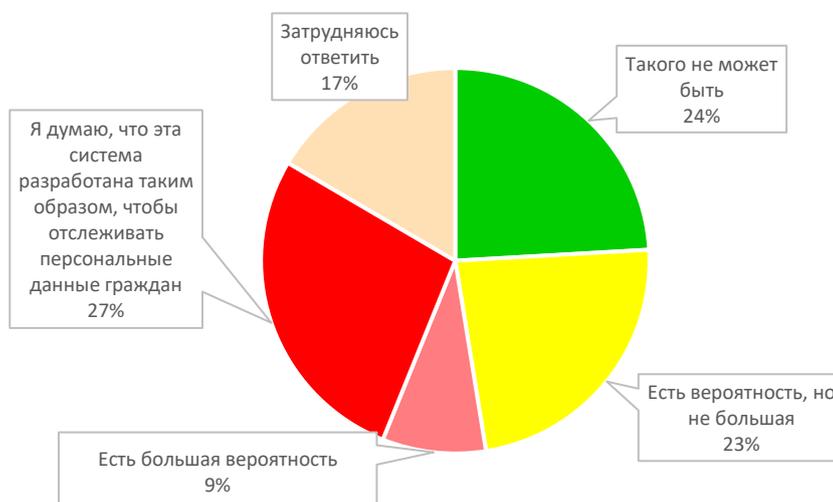
Следует отметить, что 12% респондентов отметили вариант ответа «я боюсь, что через приложение за мной могут следить государственные силовые службы» и еще 9% - вариант «я не доверяю мобильному приложению, которое разработано по заказу правительства нашей страны». То есть **в совокупности 21% респондентов не доверяют Ashyq по причине недоверия властям страны.**

Диаграмма 9. Вопрос: «По какой причине вы не доверяете системе/приложению Ashyq?»  
 Респонденты, ответившие, что не доверяют системе/приложению Ashyq, N = 228.



Еще больше недоверия системе Ashyq респонденты продемонстрировали в ответах на вопрос о риске утечки персональной информации в руки третьей стороны. Только четверть (24%) респондентов не допускают вероятность того, что персональные данные граждан, которые собираются системой Ashyq, могут быть использованы третьей стороной для каких-то других целей, не связанных с борьбой с пандемией (смотрите Диаграмму 10). Примерно столько же (23%) опрошенных считают, что такая вероятность есть, но не большая. Примерно каждый десятый (9%) опрошенный считает, что такая вероятность большая. Еще примерно четверть (27%) респондентов считают, что эта система разработана таким образом, чтобы отслеживать персональные данные граждан.

Диаграмма 10. Вопрос: «Как вы считаете, насколько вероятно то, что информация, персональные данные граждан, которые собираются системой Ashyq, могут быть использованы третьей стороной для каких-то других целей, несвязанных с борьбой с пандемией?» Все респонденты, N = 1317.



По меньшей мере **каждый десятый (13%)** опрошенный считает, что были широко распространены случаи подделки эпидемиологического статуса или доступа в общественные места в обход системы Ashyq (см. Диаграмму 11). Трое из десяти (30%) опрошенных допускают вероятность только единичных случаев, но относительное большинство (43%) респондентов считают, что таких случаев не было.

Диаграмма 11. Вопрос: «Как вы считаете, имели ли место случаи подделки эпидемиологического статуса или доступа в общественные места в обход системы Ashyq?» Все респонденты, N = 1317.



Чтобы лучше понимать, на чем основаны подозрения людей в отношении системы Ashyq и противоэпидемиологических мер в целом, респондентам был задан вопрос о том, что им лично об этом известно. 6% опрошенных заявили, что лично знают о случаях подделки эпидемиологического статуса или доступа в общественные места в обход системы Ashyq, и еще 29% сказали, что не знают лично, но слышали о таких случаях (см. Диаграмму 12). То есть **не менее трети (35%)** опрошенных знают лично или слышали о случаях подделки эпидемиологического статуса или обхода системы Ashyq.

Диаграмма 12. Вопрос: «Знаете ли вы лично случаи подделки эпидемиологического статуса или доступа в общественные места в обход системы Ashyq?» Все респонденты, N = 1317.



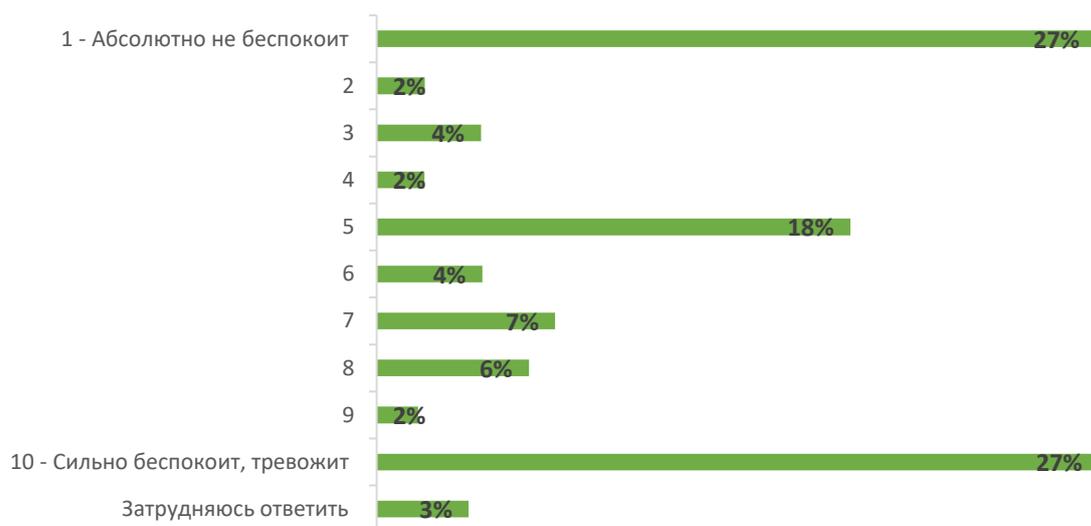
## 2.1.2. Персональные данные

Вторая часть опроса была посвящена непосредственно персональным данным: обеспокоенности их безопасностью, знаниям об их защите. В первом вопросе респонденты должны были оценить уровень своей обеспокоенности безопасностью своих персональных данных. Респондентам предлагалась сделать это по 10-балльной шкале, где «1» - «Абсолютно не беспокоит», а «10» - «Сильно беспокоит, тревожит».

27% опрошенных сказали, что их это абсолютно не беспокоит, и 27% выразили противоположную позицию – их сильно беспокоит безопасность персональных данных (см. Диаграмму 13). 22% оценили свою обеспокоенность как среднюю – «5» или «6» баллов из 10.

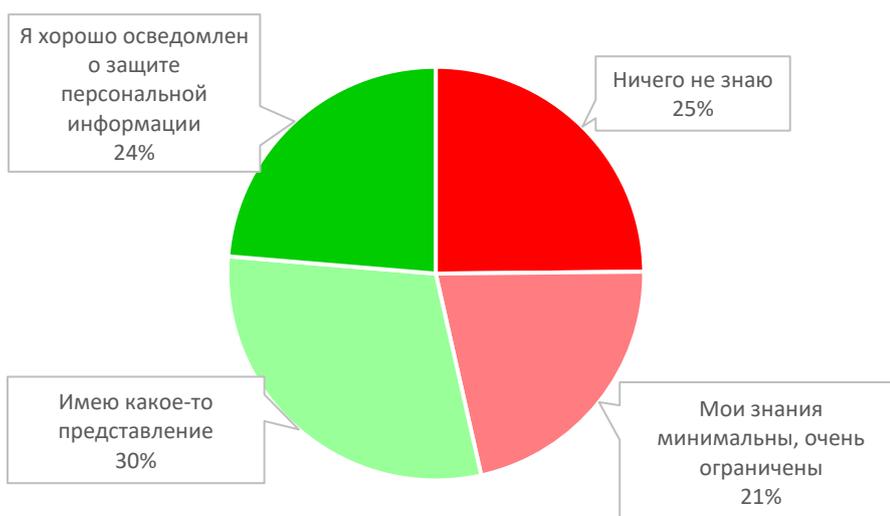
Если разделить шкалу на три зоны – отсутствие или низкий уровень беспокойства (от 1 до 4), средний уровень (от 5 до 6), высокий уровень беспокойства, тревога (от 7 до 10), то можно увидеть, что **относительное большинство (42%) опрошенных испытывают высокий уровень беспокойства.**

Диаграмма 13. Вопрос: «Насколько вас беспокоит вопрос безопасности ваших персональных данных? Оцените уровень вашей обеспокоенности по шкале от 1 до 10, где 1 – «абсолютно не беспокоит», 10 – «сильно беспокоит, тревожит». Все респонденты, N = 1317.



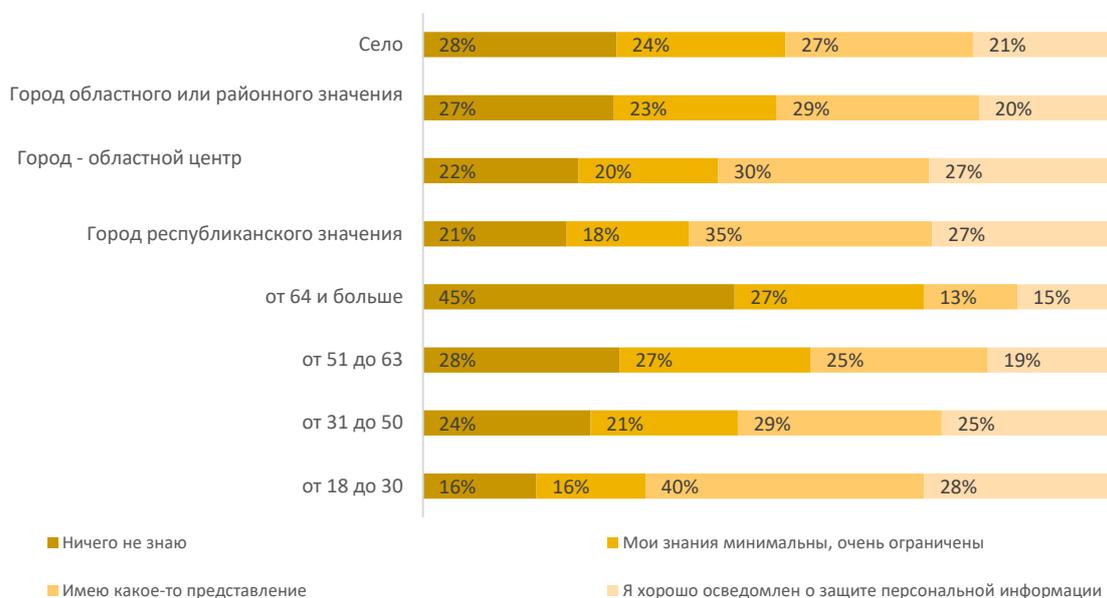
Чтобы оценить уровень осведомленности казахстанцев о защите персональных данных, респондентам был задан вопрос, где условная шкала ответов состояла из четырех делений – от «ничего не знаю» до «я хорошо осведомлен о защите персональной информации». Ответы респондентов разделились примерно на равные доли (см. Диаграмму 14). Каждый четвертый (25%) респондент сказал, что ничего не знают об этом, еще 21% респондентов сказали, что их знания минимальны, очень ограничены. Таким образом, **почти половина (46%) опрошенных имеют неудовлетворительно низкий уровень знаний о защите персональных данных.**

Диаграмма 14. Вопрос: «Как бы Вы оценили свои знания о защите персональной информации, которую вы предоставляете онлайн?» Все респонденты, N = 1317.



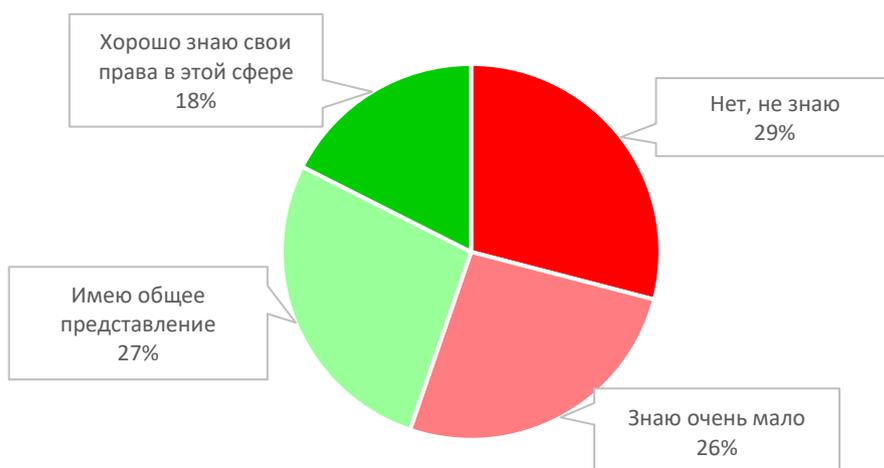
Хуже других свои знания о защите персональной информации оценивают люди в возрасте от 64 лет и старше, а также жители сел и малых городов (городов областного и районного значения). К примеру, 45% респондентов из самой старшей возрастной группы (64 года и старше) признались, что ничего не знают о защите персональной информации, которую предоставляют онлайн.

Диаграмма 15. Вопрос: «Как бы Вы оценили свои знания о защите персональной информации, которую вы предоставляете онлайн?», распределение ответов в возрастных группах и типах поселений. Все респонденты, N = 1317.



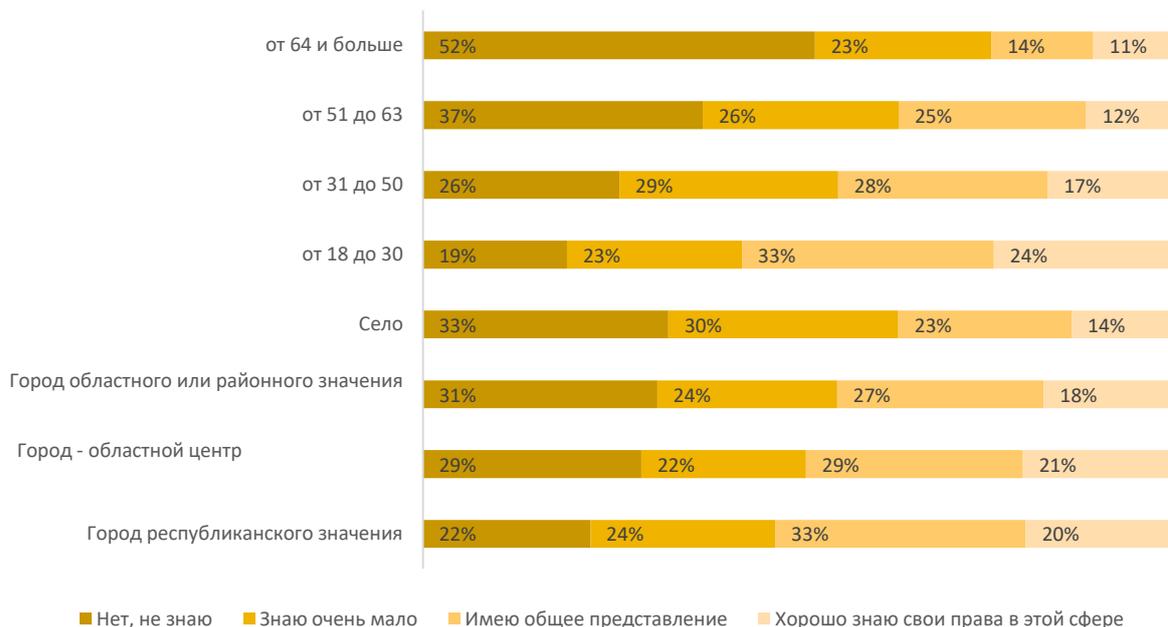
Еще в меньшей степени казахстанцы осведомлены о своих правах в сфере защиты персональной информации. Абсолютное большинство (55%) опрошенных либо не знают свои права (29%), либо знают очень мало (26%). Еще 27% респондентов заявили, что имеют общее представление, и только 18% сказали, что хорошо знают свои права в этой сфере (см. Диаграмму 16).

Диаграмма 16. Вопрос: «Знаете ли Вы свои права в сфере защиты персональной информации, которую предоставляете онлайн?» Все респонденты, N = 1317.



Если сравнивать ответы на этот вопрос в разных возрастных группах и типах поселений, то видно, что осведомленность о правах заметно ниже среди людей старшего поколения и сельских жителей (см. *Диаграмму 17*).

Диаграмма 17. Вопрос: «Знаете ли Вы свои права в сфере защиты персональной информации, которую предоставляете онлайн?», распределение ответов в возрастных группах и типах поселений. Все респонденты, N = 1317.



## 2.2 Глубинные интервью с экспертами: есть лучше, но хуже?

В рамках «качественной» части исследования были проведены глубинные интервью с экспертами и ключевыми информаторами. В данном отчете представлены результаты 12 глубинных интервью со специалистами IT, правозащитниками, сектором НПО и здравоохранения, журналистами, предпринимателями.

Целью глубинных интервью был сбор качественной информации в дополнение к опросу населения. В ходе глубинных интервью планировалось ответить на следующие вопросы.

- i. С какой целью разрабатывалась и внедрялась система Ashyq и ее мобильное приложение? Какие задачи должна была решать эта система? Рассматривались ли какие-либо альтернативы этому приложению?
- ii. Каким техническим требованиям должно было соответствовать разрабатываемое Приложение? Принимались ли во внимание какие-то (международные) стандарты, на которые следовало ориентироваться разработчикам? Были ли учтены требования защиты персональных данных?
- iii. От кого исходила инициатива? Какие организации и государственные органы были вовлечены в этот процесс? Как был организован процесс разработки Приложения?
- iv. Как принимались решения относительно разработки и внедрения Приложения, а также его характеристик? Насколько открытым был этот процесс? Были ли вовлечены в этот процесс деловые ассоциации, правозащитные организации/специалисты? Если да, то какие и какой была их позиция? Имела ли место критика на этой стадии?
- v. Какая база данных о статусе вакцинации используется в приложении? Кто является оператором этой базы данных? На основе каких сведений присваивается статус каждому гражданину (только вакцинация или есть другие критерии)?
- vi. Была ли предусмотрена система мониторинга работы Приложения? Если да, то какая и как она работала? Была ли предусмотрена система оценки результатов использования Приложения? Если да, то какие критерии оценки использовались? Какие выводы были сделаны по результатам оценки? Позволило ли приложение снять нагрузку на малый и средний бизнес и сектор здравоохранения во время борьбы с пандемией?
- vii. Имели ли место случаи жалоб или критики в отношении работы (практики использования) Приложения со стороны деловых ассоциаций, правозащитников или отдельных граждан? Если да, то в чем заключались такие жалобы/критика? Звучала ли критика приложения с точки зрения безопасности персональных данных? Что вы думаете о том, что некоторые эксперты, правозащитники и рядовые граждане считают, что государственные органы (например, фискальные) могут использовать Ashyq (данные, собранные с помощью этого приложения), для каких-то других целей, несвязанных с мерами против пандемии, например, как инструмент цифровой слежки со стороны государства?

Ниже представлено краткое резюме проведенных интервью.

Еще до появления системы «Ashyq» была разработана электронная база данных эпидемиологической информации. До того момента у Министерства здравоохранения Республики Казахстан имелась только таблица формата Excel. Здесь идея исходила от Министерства цифрового развития, инноваций и аэрокосмической промышленности. Потом была привлечена НПП «Атамекен».

*«Тогда (весна 2020 года) инициатива исходила от сообщества программистов (на волонтерских началах), которые решили помочь государству/правительству в борьбе с пандемией, в том числе Министерству здравоохранения, упорядочить имеющуюся у них эпидемиологическую информацию. И уже потом (осень 2020 года) появилась идея разработки системы Ashyq».*

Согласно официально заявленной цели, Ashyq создавался для того, чтобы помочь бизнесу работать, планировать свою работу в условиях пандемии. Владелец и главным заказчиком этого продукта является Министерство цифрового развития и аэрокосмической промышленности, также активную роль в процессе создания системы играла НПП «Атамекен».

В обсуждениях принимали участие только две стороны: разработчик и заказчик.

**Прозрачность процесса разработки и внедрения системы Ashyq была такая же, как в других подобных случаях в Казахстане, например, в случае с системой «Сергек».**

Информация эпидемиологической базы данных хранится на серверах Республиканского центра электронного здравоохранения (РЦЭЗ). Доступ к этим данным имеют только сотрудники РЦЭЗ. **Все данные зашифрованы, безопасность данных проходила соответствующие аудиты. Для этого были созданы группы программистов, хакеров на волонтерских началах.** Кроме того, проверкой занимались государственные силовые структуры. Что касается базы данных участников проекта Ashyq, то такой доступ могут иметь Министерство цифрового развития и аэрокосмической промышленности и НПП «Атамекен».

На начальной стадии рассматривалась система альтернативная той, которую в итоге приняли. Одной из особенностей альтернативного варианта была возможность определять местоположение человека с красным статусом, чтобы представители санитарно-эпидемиологических служб могли задержать его и поместить под карантин. **То есть альтернатива была еще более спорной с точки зрения соблюдения прав человека.**

Соответствие мобильного приложения общепринятым стандартам подтверждается тем, что Ashyq распространяется через сервисы «App Store» и его эквивалент «Google Play». С точки зрения безопасности персональных данных, мобильное приложение не несет серьезных рисков, риски больше связаны с человеческим фактором – людьми, имеющими непосредственный доступ к базе данных Министерства здравоохранения или НПП «Атамекен».

По признанию одного из опрошенных экспертов, ему **известно об одном случае утечки/взлома базы данных Ashyq: украденные данные были переданы/проданы для использования в коммерческих целях.**

По мнению одного из экспертов, хотя в период использования системы Ashyq в информационном пространстве можно было встретить отдельные посты блогеров, публикации в СМИ, в которых критиковалась эта система, **широкой общественной дискуссии по этому поводу не было.** Какой-либо консолидированной позиции правозащитников в отношении системы Ashyq также не наблюдалось. Тем не менее, система вызывает вопросы с точки зрения соответствия правовым нормам. По мнению

правозащитников, **система Ashyq была разработана и внедрена таким же образом, как в свое время это было сделано с «Сергек» - никакого обсуждения, «просто навязали».**

Во-первых, это вопросы обеспечения безопасности персональных данных (тайны личной жизни). Никто не спрашивал мнение общества, не было никакой общественной (открытой) дискуссии о том, как будет обеспечена безопасность персональных данных, какие именно сведения будут собираться. В правовых странах действует стандарт сбора, хранения и использования персональных данных, предоставляемых онлайн (GDPR).

*«Нашему правительству не нужно ничего изобретать, достаточно следовать европейскому стандарту GDPR».*

Во-вторых, это вопросы монополии на использование этой базы данных. Кто решил, где и каким образом будет храниться вся собираемая информация, как она будет использоваться? Такие базы данных могут представлять большой интерес для коммерческих структур и их стоимость может оцениваться большими суммами, что создает потенциал для коррупции, когда этими базами данных оперируют государственные органы.

Предприниматели рассказывают о том, что, хотя идея проекта Ashyq выглядит разумной и полезной, **на практике ее реализация сопровождалась многочисленными примерами нарушений или двойных стандартов.** Предприниматели задавались вопросами: почему одни предприятия должны были работать с Ashyq, а другие могли работать без него? Почему торгово-развлекательные центры должны были работать с Ashyq, а базары могли работать без нее? Почему одни магазины работали до 23:00 или даже дольше, а другие заведения строго соблюдали правила?

Предприниматели сомневаются, что система Ashyq действительно способствовала сдерживанию пандемии. Иными словами, эта система не решала задачи, которые была призвана решать. Их отношение к этой системе такое же, как и к другим карантинным мерам правительства, принятым во время пандемии.

*«Им нужно было что-то предложить, вот они и придумали этот «Ашык»».*

Специалисты IT дают системе Ashyq положительную оценку, объясняя это тем, что ее разработка и внедрение являются хорошим опытом для казахстанской индустрии IT, своевременным решением, которое помогло бизнесу функционировать во время пандемии. А риски, связанные с безопасностью персональных данных, в данном случае такие же, как и в любой другой базе данных, которой управляют государственные органы.

Правозащитники оценивают систему скорее негативно («между негативно и нейтрально, но скорее негативно»), поскольку, по их мнению, это очередной пример того, как **государство принимает решение без открытого обсуждения с обществом, не обращая внимания на нарушения правовых норм.**

Предприниматели оценивают систему Ashyq неоднозначно. С одной стороны, эта система стала хотя бы каким-то «понятным» правилом, по которому можно было работать в условиях карантинных мер. С другой, они разделяют сомнения тех, кто не верит, что эта система действительно способствовала сдерживанию пандемии. Многие торговые точки

(маленькие магазины, базары) работали без Ashyq, а многие рестораны использовали эту систему чисто формально (имели QR-код, но пропускали всех посетителей без исключения).

## Выводы и рекомендации

Отвечая на вопрос «что дальше после 12-месячного использования Ashyq?», вырисовывается неопределенная картина. Во-первых, остаются непонятными следующие моменты, на которые важно ответить самим государственным органам, чтобы двигаться дальше:



Насколько соразмерным и необходимым было внедрение мобильного приложения Ashyq, чтобы противостоять распространению коронавируса в Казахстане и стабилизировать эпидемиологическую ситуацию особенно в моменты «наихудшего сценария» с 7,500 случаев в сутки и выше.



Насколько эффективным и результативным стало приложение в качестве помощника министерства здравоохранения в сдерживании распространения COVID-19 в сравнении с другими «ручными» мерами («ручной» ввод данных, мониторинговые группы, штрафы и пр.); какие были ожидаемые результаты от внедрения этого приложения.



Насколько прозрачным и понятным было данное решение для всех, включая бизнес, общественность и государственные органы.



Что будет дальше с приложением: будет ли оно использоваться дальше или будет модифицировано с целью дальнейшего внедрения в сектор здравоохранения (е-здравоохранение) для достижения целей и задач в рамках Цифрового Казахстана.



Что будет с базой данных, собранной в процессе работы приложения на протяжении года (все данные по ПЦР, вакцинации, статусах граждан): кто будет иметь доступ (помимо Министерства цифрового развития, инноваций и аэрокосмической промышленности, Министерства здравоохранения, НПП Атамекен, МВД), когда эти данные будут удалены.



Проведут ли Министерство цифрового развития, инноваций и аэрокосмической промышленности и Министерство здравоохранения мониторинг и оценку работы приложения: с момента разработки, внедрения в эксплуатацию и завершения проекта; какие ошибки и уроки извлекут (помимо технических и коррупционных), будут ли они представлены в публичном доступе с целью улучшения дальнейших электронных сервисов в стране.



Когда заработает закон «О персональных данных и их защите» и профильный орган сможет фиксировать все нарушения, происходящие по вине

других государственных органов, имеющих доступ к информационным базам данных и продолжающих собирать все больше данных, когда речь идет о здоровье людей.



Собираются ли профильные государственные органы выстраивать коммуникационную стратегию с казахстанцами для повышения доверия к принимаемым мерам.

Во-вторых, анализ публикаций в медиа, результатов опроса и глубинных интервью показал **отсутствие системности, прозрачности, коммуникационной стратегии со стороны государственных органов, отвечающих за приложение Ashyq с момента разработки, на пути внедрения и до момента отказа от приложения как санитарно-эпидемиологической меры**. Несмотря на, казалось бы, положительный опыт для IT-индустрии страны в целом, о котором говорили в интервью технические специалисты и разработчики, основное внимание уделялось критике работы приложения на первых месяцах. Многочисленные технические ошибки (невозможность загрузить приложение или войти в него после скачивания, ошибочная идентификация, идентификация третьей стороной, медленная интеграция с другими базами данных) на первых парах действовали дополнительным раздражающим фактором для предпринимателей и граждан, пока Ashyq не интегрировали с другими сервисами, в частности онлайн банкингом (Kaspi, Halyk) и eGov мобильным приложением. Очевидно, что **Ashyq останется одним из сервисов в системе здравоохранения с полной интеграцией соответствующих баз данных, а не в качестве самостоятельного приложения**.

Вместе с тем, если учитывать тот факт, что могли принять менее прозрачную версию приложения, которая могла определять местоположение человека с красным статусом, чтобы представители санитарно-эпидемиологических служб могли задержать его и поместить под карантин, то на деле ситуация с точки зрения соблюдения прав человека оказалась непонятной. Хотя с точки зрения соблюдения критериев международного права для ограничения прав и свобод человека внедрение приложения Ashyq не было соразмерным и необходимым, поскольку, с одной стороны, отсутствуют полноценные данные в разрезе «ручной» ввод vs мониторинговые группы vs маски vs Ashyq vs ограничение работы субъектов бизнеса, чтобы понимать, какая мера сыграла какую роль, а с другой стороны имеющиеся ограниченные данные по количеству проверочных рейдов и предотвращенным заражениям или распространению COVID-19 никак не соотносятся, поскольку их корреляция не является прямой.

Если подвести итоги и попытаться отделить зерна от плевел, тогда ситуация становится более или менее понятной. Само приложение Ashyq как приложение оказалось технически слабым, требовало доработки с учетом различных особенностей – *возрастных* (кто может пользоваться приложением – дети до 18 лет, которые болели коронавирусом, вообще выпали из категории, потому что у родителей не обновлялся статус на контактного, возрастная группа 50+ лет), *технических* (у кого есть смартфон и кто может им пользоваться, наличие мобильного интернета и связи), *социальных* (невозможность пользоваться приложением теми, кто был осужден по определенным статьям Уголовного кодекса РК, в частности экстремизм и терроризм, из-за блокировки их ИИН), *юридических*

(если было известно об утечке персональных данных из Ashyq, почему об этом публично не говорят и не наказывают виновных в соответствии с законом о персональных данных), *коррупционных* (ввод данных для третьего лица, Print Screen статуса, «ручная» проверка по ИИН). Тем не менее, **так или иначе оно выполнило свою функцию в помощи объектам бизнеса работать в условиях карантина, однако провалилось в части информационно-коммуникационной работы с гражданами.**

В-третьих, по факту реализации карантинных мер, включая приложение Ashyq, возникало много вопросов и фиксировались **многочисленные примеры нарушений и двойных стандартов**. Предприниматели задавались вопросами: почему одни предприятия должны были работать с Ashyq, а другие могли работать без нее? Почему торговоразвлекательные центры должны были работать с Ashyq, а базары могли работать без нее? Почему одни магазины работали до 23:00 или даже дольше, а другие заведения строго соблюдали правила? Почему (маленькие магазины, базары) работали без Ashyq, а многие рестораны использовали эту систему чисто формально (имели QR-код, но пропускали всех посетителей без исключения), в частности в крупных городах?

С точки зрения обеспечения медицинского контроля и здравоохранения ситуация менее понятной. **«Цифровая слежка» по снижению контактов, контролю заболевания, передвижению и скоплению зараженных COVID-19 не помогла и не принесла ощутимых результатов из-за недоверия и попустительского отношения граждан и коррупции контролирующих органов - мониторинговых групп, чиновников на местах и охранников объектов массового скопления людей.**

Наконец, стоимость разработки и внедрения Ashyq – небольшая (приложение было бесплатно передано Министерству цифрового развития, инноваций и аэрокосмической промышленности). Однако наибольшая часть расходов была связана с информированием населения в процессе внедрения приложения, которое, по сути, провалилось в силу обозначенных проблем и трудностей. Цитата Комитета санитарно-эпидемиологического контроля, который призывал «всех казахстанцев соблюдать карантинные требования и надеялся на то, что административные штрафы позволят взять под контроль распространение среди населения опасных инфекционных заболеваний, таких как COVID-19»<sup>65</sup>, по крайней мере показывает низкую эффективность принимаемых мер.

Для граждан, как показала практика, мало кто понимал, что такое Ashyq. Люди говорили про QR-код, а не приложение. Более того, многие ушли сразу в мобильное приложение Kaspi из-за удобства в обмен на доступ к сервисам, продукции, услугам и соглашаясь на передачу персональных данных третьим лицам (банкам) посредством интеграции баз данных. Кроме того, **для рядовых граждан Ashyq вызывал больше вопросов из-за того, что система использовалась не повсеместно и не одинаково строго в разных городах и разных заведениях.** Например, в малых городах, в сельской местности эта система была не так широко распространена, как в крупных городах, поэтому гипотеза о том, что Ashyq помог цифровизации и повышению цифровой грамотности и продвижению культуры защиты персональных данных и кибергигиены не подтвердилась.

<sup>65</sup> [Больных COVID-19 казахстанцев будут наказывать за нарушение самоизоляции: 07 июня 2021, 10:25 - новости на Tengrinews.kz.](#)

Как показали результаты опроса, три четверти взрослого населения страны пользовались системой Ashyq, а те люди, которые этого не делали, являются преимущественно жителями сел или малых городов, где общественные места, участвовавшие в проекте Ashyq, встречались редко. Также среди тех, кто не пользовался этой системой, большую долю составляют люди старшего поколения – старше 50 лет.

Недоверие системе Ashyq и ее мобильному приложению слабо распространено. А те, кто не доверяет этой системе, объясняет это не обеспокоенностью проблемой безопасности персональных данных, а сомнениями в том, что эта система способствовала сдерживанию пандемии, как это заявлялось правительством.

Многие опрошенные допускают вероятность использования этой системы в целях, несвязанных с заявленными – борьбой с распространением пандемии, например, в целях слежки за людьми со стороны силовых структур. Значительная доля опрошенных обеспокоена безопасностью персональных данных, предоставляемых онлайн.

Как и два предыдущих исследования в 2020–2021 годах, данный опрос общественного мнения продемонстрировал, что уровень осведомленности в вопросах защиты персональных данных и правах в этой сфере остается на очень низком уровне, что по факту означает повышенную уязвимость казахстанцев в киберсреде.

Безусловно, однозначных ответов на многие вопросы не будет и быть не может, к этому нужно быть готовым. Во всем мире пилотное внедрение технологий цифрового отслеживания контактов сталкивалось с критикой, техническими ошибками и правовыми коллизиями, однако открытость и признание проблем позволило немного сгладить ситуацию и выстраивать доверие между правительствами, IT-компаниями и гражданами в такое нестабильное время, требующее новаторских, незамедлительных, но качественных решений<sup>66</sup>.

---

<sup>66</sup> [Эффективны ли технологии цифрового отслеживания контактов во время вспышек инфекционных заболеваний? | Cochrane.](#)