НАБОР ИНСТРУМЕНТОВ ДЛЯ ПРИЛОЖЕНИЙ COVID-19

Как **законодательным и директивным органам, разработчикам приложений, операторам приложений, заинтересованным государственным организациям и представителям широкой общественности**

внести свой вклад в развитие системы сдержек и противовесов и обеспечить соответствие целевому назначению инструментов, развертываемых во время пандемии?

Содержание

Введение

Пандемия Covid-19 побудила правительства многих стран ввести различные меры: от традиционных санитарно-эпидемиологических, таких как масочный режим и социальное дистанцирование, до ряда беспрецедентных технологических решений, таких как использование приложений по отслеживанию контактов и цифровых паспортов иммунизации.

Проект Covid App Project представляет собой двухэтапную инициативу общественных организаций, обусловленную научным интересом к мерам по противодействию распространению коронавирусной инфекции.

Фаза 1 проекта охватывала изучение опыта применения приложений по отслеживанию контактов в Бразилии, Колумбии, Индии, Иране, Ливане и ЮАР до июля 2021 года, рассматривались результаты их применения с точки зрения эффективности в качестве мер общественного здравоохранения, анализировались функциональная избыточность и непреднамеренные последствия их применения, такие как ограничение доступа к общественной жизни. Этот общий исследовательский интерес объединил усилия шести некоммерческих организаций: ALT Advisory (ЮАР), Internet Democracy Project (Индия), InternetLAB (Бразилия), Karisma (Колумбия), SMEX (Ливан), и United for Iran (Иран). Агентство AWO осуществляло координационную поддержку.[1]

Фаза 2 проекта охватывает приложения, разработанные с июля 2021 года, главным образом т.н. паспорта иммунизации (демонстрирующие статус вакцинации, результаты тестов или сертификаты о статусе переболевшего). Это исследование, основанное на техническом обзоре глобально репрезентативной выборки приложений, рассматривает тенденции в политических, правовых и технических подходах по всему миру посредством анализа и технической оценки 11 связанных с Covid-19 приложений, разработанных (или внедренных) в первую очередь органами государственной власти, а также в отдельных случаях и другими организациями в Австралии, Бахрейне, Чили, Индонезии, Израиле, Нидерландах, Тунисе и штате Западная Австралия.

Указанные страны были отобраны с целью обеспечения репрезентативности различных континентов и регионов, а также для того, чтобы отразить основные тренды, выявленные в ходе исследования. Также в рамках исследования проводилось изучение приложений, которые можно считать глобально значимыми: CommonPass некоммерческой организации WEF и Travel Pass ассоциации IATA.

Результаты второй фазы исследований:

- Отчет “Приложения Covid-19: политические, правовые и юридические тренды“ (именуемый в дальнейшем “Отчет по трендам”)[2]. В отчете представлены результаты исследования фазы 2 и соответствующие рекомендации. В нем рассматриваются подходы к разработке приложений и их практическому

[1] https://www.awo.agency/latest/covid-19-app-project/

[2] https://awo.agency/files/Covid-Apps-Policy-Legal-Tech-Trends.pdf

применению с позиции анализа пользы для общественного здравоохранения, а также вопросы функциональной избыточности и непреднамеренных последствий для отдельных граждан. На основе этого анализа для заинтересованных сторон подготовлены ряд рекомендаций и описание передового опыта с целью последующего использования для разработки эффективных и устойчивых практик общественного здравоохранения.

- "Отчет о рисках конфиденциальности приложений COVID-19 (Часть II)" (именуемый в дальнейшем "Технический отчет")[3]. Отчет содержит подробные результаты технического анализа одиннадцати выбранных приложений на предмет соответствия передовым практикам в областях защиты персональных данных, включая, помимо прочего, соответствие концепциям проектируемой конфиденциальности и минимизации данных. Также в нем приведены рекомендации о том, как лучше всего обеспечить эффективность и безопасность приложений Covid-19.

- "Набор инструментов для приложений Covid-19" (именуемый в дальнейшем "Набор инструментов")[4]. Это документ, сформированный на основе результатов и рекомендаций как Технического отчета, так и Отчета по трендам. Он также включает и использует результаты исследований, полученных в ходе Фазы 1 проекта Covid, реализованного шестью вышеперечисленными некоммерческими организациями. В целом, документ содержит всестороннее описание передового опыта, доступные методические указания, а также инструменты внедрения для всех заинтересованных сторон, задействованных в мерах по борьбе с пандемией коронавирусной инфекции или заинтересованных в осуществлении таких мер: сотрудников законодательных и директивных органов, разработчиков приложений, операторов приложений, осуществляющих приемку уполномоченных государственных организаций и широкой общественности.

Рекомендации, представленные в настоящем Наборе инструментов, предназначены для усиления мер по предотвращению распространения инфекции и обеспечения их эффективности с точки зрения общественного здравоохранения. Они также направлены на предоставление практических указаний для заинтересованных сторон, задействованных в борьбе с пандемией, для предотвращения функциональной избыточности приложений и непреднамеренных последствий при использовании высокотехнологичных решений. Настоящий набор инструментов представляет собой базовые рекомендации на основе передового опыта, при этом заинтересованные стороны могут принять решение доработать его таким образом, чтобы учесть и проработать все дополнительные вопросы, характерные для их ситуации.

Несмотря на то, что рекомендации структурно разделены по группам непосредственно вовлеченных заинтересованных сторон (например, отдельные рекомендации для директивных и законодательных органов), все они актуальны для всех остальных заинтересованных сторон.

[3] https://awo.agency/files/Covid-19-Apps-Technical-Review-2022.pdf
[4] https://awo.agency/files/covid-app-toolkit-en.pdf

Кроме этого, широкой общественности может быть полезно ознакомиться с трендами и рекомендациями, представленными в данном Наборе инструментов, с целью повысить свою осведомленность в затрагивающих их интересы вопросах (например, на что именно следует обращать внимание при прочтении политики конфиденциальности приложения Covid-19). Для дальнейшего содействия информированию, каждый из двух разделов данного набора инструментов начинается с краткого резюме для конечных пользователей. Цель резюме – прояснить, чего можно ожидать широкой общественности от сторон, задействованных в реагировании на пандемию. Сюда входят ожидания в части подхода, основанного на принципе пропорциональности, уважение прав и обеспечение эффективности с точки зрения общественного здравоохранения.

Для обеспечения глобального охвата, Набор инструментов доступен дополнительно на семи языках:

- Арабском[5]
- Фарси[6]
- Французском[7]
- Хинди[8]
- Португальском (Бразилия)[9]
- Русском[10]
- Китайском (упрощенное письмо)[11]
- испанский[12]

[5] https://awo.agency/files/covid-app-toolkit-ar.pdf
[6] https://awo.agency/files/covid-app-toolkit-fa.pdf
[7] https://awo.agency/files/covid-app-toolkit-fr.pdf
[8] https://awo.agency/files/covid-app-toolkit-hi.pdf
[9] https://awo.agency/files/covid-app-toolkit-pr.pdf
[10] https://awo.agency/files/covid-app-toolkit-ru.pdf
[11] https://awo.agency/files/covid-app-toolkit-zh.pdf
[12] https://awo.agency/files/covid-app-toolkit-es.pdf

1. Рекомендации для законодательных и директивных органов

Чего общественность может ожидать от сторон, задействованных в борьбе с пандемией, и почему?

Директивные и законодательные органы могут внедрять политику и законодательную базу на основе соответствующих консультаций и рекомендаций сообщества общественного здравоохранения. Для общественности важно понимать, что введение таких рамок и гарантий нацелено на обеспечение со стороны директивных и законодательных органов эффективности общественного здравоохранения при соблюдении пропорционального подхода. Такой подход приведет к созданию и предоставлению эффективных гарантий при разработке и использовании приложений Covid-19, с применением передового международного опыта, уважающего права граждан. На практике, если приложение Covid используется страной в качестве элемента борьбы с пандемией, эффективность такого приложения с точки зрения общественного здравоохранения может стать частью более широкой скоординированной стратегии по борьбе с распространением Covid-19, имеющей ключевое значение для предотвращения непреднамеренных последствий.

Конечные пользователи приложений Covid-19, в том числе уязвимые сообщества, такие как беженцы и рабочие-мигранты, должны иметь доступ к жизненно важным услугам. Чтобы обеспечить целостную стратегию общественного здравоохранения, которая способствует доверию, доступна и понятна населению, приложения должны быть составной частью более широкой стратегии, основанной на фактических данных. Это означает, что внедрение приложений должно координироваться между различными ветвями власти на федеральном и местном уровнях и основываться на глобальных технических стандартах, а их использование должно сочетаться с инициативами по тестированию и отслеживанию, изменениями в социальной политике и политике общественного здравоохранения, такими как социальное дистанцирование. Четкое и скоординированное использование приложения должно сочетаться с информационно-разъяснительной работой в средствах массовой информации (и социальных сетях), повышающей осведомленность общественности о приложении и уровень ее информированности.

В конечном итоге, общественность должна иметь предпосылки доверять предпринимаемым правительством мерам, что подразумевает все вышеперечисленное, а также усилия по предотвращению избыточности функционала и непреднамеренных последствий. Этого можно достичь путем разработки и внедрения соответствующих правовых режимов, прозрачности использования данных и соглашений об обмене данными, предназначенных исключительно для поддержки стратегии общественного здравоохранения, а не для достижения других политических или стратегических целей. Доверие дополнительно можно укрепить путем обеспечения равноправного применения мер общественного здравоохранения по всей стране с независимыми механизмами надзора, созданием нецифровых альтернатив или иным путем, предотвращающим наказания за неиспользование приложений.

<table>
<tr><th colspan="3">Эффективность в здравоохранении</th></tr>
<tr><td colspan="3">Тренд 1</td></tr>
<tr><td rowspan="3">Приложения по отслеживанию контактов и технологические меры применяются в странах с ограниченным или неравным уровнем доступа к интернету и мобильным технологиям</td><td>Оценка</td><td>Правительства многих стран, невзирая на существовавшее ранее неравенство в отношении доступа к интернету и мобильным технологиям, ввели технологические меры в целях борьбы с распространением Covid-19. Значение этой проблемы невозможно переоценить, поскольку неравный доступ к технологиям, связанным с использованием смартфонов, может усугубить существующее неравенство и вызвать вопросы этического характера. Кроме того, при предоставлении услуг социального обеспечения преимущественно через онлайн-платформы, уязвимые сообщества, которые чаще всего имеют ограниченный доступ к интернету и не имеют мобильных устройств, могут быть лишены доступа к жизненно важной помощи.</td></tr>
<tr><td>Рекомендация</td><td>Центральные органы власти должны поддерживать доступ к жизненно важным услугам для уязвимых групп населения (особенно беженцев и рабочих-мигрантов).</td></tr>
<tr><td colspan="2">Как внедрить рекомендацию?</td></tr>
<tr><td></td><td colspan="2">□ Органы государственной власти могут провести оценку текущего состояния и распределения критической интернет-инфраструктуры в стране с целью выявления областей, нуждающихся в развитии.</td></tr>
</table>

	□ Провести инвестиции в критически важную интернет-инфраструктуру в выявленных областях, нуждающихся в развитии. Сюда можно отнести субсидирование тарифных планов мобильной связи, предоставление бесплатных точек доступа Wi-Fi и даже программы цифровой грамотности.

<table>
<tr><th colspan="3">Эффективность в здравоохранении</th></tr>
<tr><td colspan="3">Тренд 2</td></tr>
<tr><td rowspan="3">Приложения зачастую не имели связи с более широкими ответными мерами общественного здравоохранения и характеризовались низким уровнем использования</td><td>Оценка</td><td>Судьба приложений по отслеживанию контактов тесно связана с несогласованностью ответных мер на пандемию на национальном и местном уровнях. Некоторые приложения были изолированы от довольно спорадической стратегии общественного здравоохранения, и правительства не уделяли приоритетного внимания эффективному использованию полученных данных. Это также означало, что приложения и другие меры технологического характера не были согласованы с потребностями системы здравоохранения, что особенно наглядно проявилось в отсутствии обмена данными между центральными и местными органами власти. Это привело к утверждениям, что принятие приложений по отслеживанию контактов в некоторых странах было просто упражнением для галочки, чтобы показать, что правительство задействовало технологические решения для борьбы с пандемией.</td></tr>
<tr><td>Рекомендация</td><td>Центральные органы власти должны разработать единый государственный механизм реагирования на Covid-19 (или любую другую пандемию), затрагивающий органы власти как общегосударственного, так и регионального уровня.</td></tr>
<tr><td colspan="2">Как внедрить рекомендацию?</td></tr>
<tr><td colspan="2">□ Центральные органы власти имеют возможность встроить приложения по отслеживанию контактов в более широкую инфраструктуру общественного здравоохранения. Приложения наиболее функциональны, когда они используются наряду с традиционными системами для отслеживания контактов, которые, в свою очередь, зависят от наличия достаточного потенциала тестирования и персонала местных, региональных и национальных учреждений</td></tr>
</table>

	здравоохранения. □ Для обеспечения пропорционального и эффективного реагирования общественного здравоохранения следует применять стратегию, основанную на фактических данных.

<table>
<tr><th colspan="3">Эффективность в здравоохранении</th></tr>
<tr><td colspan="3">Тренд 3</td></tr>
<tr><td rowspan="3">Развертывание многочисленных и многоцелевых приложений</td><td>Оценка</td><td>В ряде стран получили распространение различные приложения по отслеживанию контактов. В частности при участии в разработке отдельных региональных органов власти было выпущено несколько приложений с различной функциональностью. Правительства некоторых государств использовали приложения с функциями, выходящими за рамки отслеживания контактов, такими, как предоставление удаленного медицинского обслуживания. В некоторых случаях это было следствием ограниченной межведомственной координации и децентрализации систем общественного здравоохранения. Многочисленность официальных приложений по отслеживанию контактов в условиях Covid-19 в некоторых странах, возможно, ослабило глубину их внедрения в целом.</td></tr>
<tr><td>Рекомендация</td><td>Органы государственной власти должны разработать единый государственный подход к реагированию на пандемию, затрагивающий органы власти как национального, так и регионального уровней.</td></tr>
<tr><td colspan="2">Как внедрить рекомендацию?</td></tr>
<tr><td colspan="3">□ Обеспечить согласованность реакции государственных структур и органов здравоохранения.</td></tr>
</table>

	□ Использовать мировые образцы передовой практики при разработке приложений по отслеживанию контактов, такие как интерфейс GAEN (Google Apple Exposure Notification) API, что способствует развитию надежной инфраструктуры.

Эффективность в здравоохранении		
Тренд 4		
Недостаток общественного доверия и осведомленности сказывается на приложениях по отслеживанию контактов	**Оценка**	Во всех рассматриваемых странах внедрению приложений по отслеживанию контактов препятствовало либо отсутствие общественного доверия, либо низкая осведомленность населения. Отчасти это объясняется слабой агитационной работой в отношении приложений, в том числе отсутствием целенаправленных и адресных информационных сообщений со стороны правительства. Кроме того, некоторые приложения столкнулись с проблемами, связанными с нарушением неприкосновенности частной жизни, включая злоупотребления полномочиями по негласному наблюдению со стороны правоохранительных органов и спецслужб в ряде стран, что повлияло на мнение журналистов, лидеров оппозиции, судей и правозащитников.
	Рекомендация	Органы государственной власти должны развивать взаимодействие со средствами массовой информации. Контент, предназначенный для повышения осведомленности и просвещения общественности, должен быть научным и подаваться профессионально.
	Как внедрить рекомендацию?	
	□ Приложения по отслеживанию контактов могут принести существенную пользу только в том случае, если люди знают об их существовании и доверяют им, не опасаясь за нецелевое использование своих персональных данных всеми вовлеченными в процесс участниками и заинтересованными сторонами.[12] Использование международных	

	передовых практик при разработке приложений предотвращает проблемы функциональной избыточности и утечки данных, повышая тем самым готовность населения использовать приложение. □ Информировать людей о существовании приложения и поощрять его использование на различных уровнях правительства, органов здравоохранения, средств массовой информации и предприятий частного сектора.

Эффективность в здравоохранении		
Тренд 5		
Альтернативные меры зачастую оказывают бóльший эффект на общественное здравоохранение, чем приложения по отслеживанию контактов	**Оценка**	Несмотря на то, что приложения по отслеживанию контактов привлекают много внимания и вызывают общественную дискуссию, альтернативные им меры часто носят более масштабный характер. Некоторые страны в основном полагались на массовый скрининг, целевое тестирование и карантинные меры, что потребовало мобилизации медицинских работников для проведения обследования миллионов людей. Национальный режим изоляции и карантинные меры также сыграли важную роль в сдерживании распространения Covid-19.
	Рекомендация	Органы государственной власти должны разработать меры реагирования на пандемию, не основанные на технологиях, в качестве альтернативы техническим мерам реагирования с использованием приложений.

	Как внедрить рекомендацию?
	□ Укреплять сотрудничество и координацию между государственным и частным секторами для обеспечения готовности больниц и внедрять приложения по отслеживанию контактов в более широкую стратегию общественного здравоохранения, включающую эпидемиологические расследования и доступное тестирование. □ Обеспечить проведение социальной политики, позволяющей (потенциально инфицированным) людям следовать правилам и рекомендациям, например, предотвращать наступление бедности в результате пандемии путем предоставления экономической поддержки во время карантина или изоляции. □ Обеспечить доступность средств индивидуальной защиты для населения (например, масок).

Функциональная Избыточность и Непредвиденные Последствия		
Тренд 1		
Ограниченное обращение к законодательству о чрезвычайных ситуациях, расширенное использование чрезвычайных полномочий	**Оценка**	Не все страны, в которых проводилось исследование, объявили режим чрезвычайной ситуации во время проведения исследования. В тех случаях, когда это было сделано, правовая основа для реализации различных мер вытекала из конкретных положений конституции или законодательной базы страны. Обычно это означает, что при соблюдении определенных условий и правил государство может осуществлять полномочия, отступая от обычных стандартов в области прав человека. Однако чрезвычайное положение может негативно повлиять на некоторые уязвимые сообщества, особенно в тех случаях, когда принятые меры закрепляют и усугубляют существующую дискриминационную практику. В странах, не объявлявших чрезвычайное положение, наряду с обычными законодательными нормами использовались чрезвычайные полномочия. Такая ситуация отличается от объявления чрезвычайного положения тем, что в основе полномочий лежит уже существующее законодательство, как правило, законы об общественном здравоохранении, позволяющие реализовывать определенные меры без привязки к чрезвычайной ситуации. Это не всегда соответствует прямым положениям конституции или законодательной базы и, следовательно, создает возможность осуществления широких полномочий без соответствующих сдержек и противовесов.

	Рекомендация	Органы государственной власти должны внедрять меры в сфере здравоохранения на основании соответствующих правовых инструментов, предусматривающих эффективные гарантии прав человека, в том числе, когда они основаны на правомерном объявлении чрезвычайной ситуации. В будущем при возникновении кризисов, органы государственной власти должны проводить оценку влияния на права человека, которая послужит основой для создания правовой базы. Эта работа должна включать анализ последствий введения чрезвычайного положения и состояния бедствия, а также определение мер, которые можно считать необходимыми и оправданными. В рамках процесса, аналогичного тому, который задействуется для устранения серьезных нарушений прав человека, может быть целесообразно использовать переходные механизмы, которые на базе оценки практик и норм, использованных во время пандемии Covid-19, привели бы в будущем к улучшению подотчетности и реорганизации с тем, чтобы исключить необходимость использования экстраординарных мер.
	Как реализовать эту рекомендацию?	
	□ Принять законы и утвердить механизмы реагирования на случай новой волны Covid-19 или иной пандемии с целью ограничения необходимости введения чрезвычайного положения. □ Если для быстрого реагирования требуется введение чрезвычайного положения, необходимо предусмотреть положение о временных рамках, согласно которому новые меры в области общественного здравоохранения должны быть строго ограничены по времени.	

	□ Провести оценку воздействия на права человека существующих (и перспективных) законов о здравоохранении до того, как возникнет необходимость в их применении. Оценки воздействия на права человека должны проводиться прозрачно, чтобы обеспечить как надлежащую добросовестность, так и общественное доверие. □ Законодательный процесс должен базироваться на фактических данных, в этом случае можно гарантировать пропорциональность и эффективность реакции системы общественного здравоохранения. Следует предотвратить длительные периоды чрезвычайных положений путем использования лучших мировых практик в области оценки стратегии и влияния, а также использования демократических процессов утверждения и надзора.

Избыточность Функционала и Непредвиденные Последствия		
Тренд 2		
Страны имеют слабые, а иногда и не имеющие законной силы механизмы защиты данных	**Оценка**	В выводах по Фазе 1 говорится, что законы о защите данных во время пандемии либо пока не вступили в силу, либо все еще находятся на стадии законотворческого процесса, либо никогда не существовали вовсе. В общем случае, более надежные механизмы защиты данных могут усилить надзор во всех странах исследования.
	Рекомендация	Органы государственной власти должны ускорить процесс введения в действие законов о защите данных с необходимыми положениями, охватывающими все приложения и информационные системы, связанные с Covid-19. Правительства и их частные партнеры должны обеспечить основанную на правах человека и прозрачную нормативную и директивную базу, уделяя особое внимание правам на неприкосновенность частной жизни. Законодательство в области защиты данных должно быть пересмотрено и согласовано с любыми отдельно действующими законами о защите данных.
	Как реализовать эту рекомендацию?	

Функциональная Избыточность и Непредвиденные Последствия		
Тренд 3		
Увеличенный и непрозрачный обмен данными между государственными структурами	**Оценка**	Сбор и обмен данными государственными органами в ответ на пандемию является обычной практикой для правительств во всем мире. Основной причиной для этого является необходимость регулирования и удовлетворение запросов на передвижение внутри страны во время действия карантинных мер. Это предполагает объединение ранее существовавших баз данных, а также баз данных, созданных специально для противодействия Covid-19. При этом отсутствие законов о защите данных или других нормативных актов приводит к функциональной избыточности приложений и неблагоприятному воздействию на некоторые уязвимые сообщества в результате обмена конфиденциальными личными данными с правоохранительными органами, а также ограничения свободы передвижения тех, кто, как правило, не имеет доступа к онлайн-платформам для подачи заявлений на получение разрешений на поездки.
	Рекомендация	Органы государственной власти и частные организации, сотрудничающие в области обработки персональных данных в условиях пандемии, должны подготовить и опубликовать отчеты о воздействии на права человека в целях поддержания транспарентности и подотчетности.

		Все приложения должны сопровождаться юридически необходимыми документами, такими как условия предоставления услуг и политика конфиденциальности, причем эти документы должны находиться в открытом доступе. Предоставлять точную информацию о том, какие данные собираются и с какой целью, где и как долго данные будут храниться, кому и в каких целях будут передаваться, а также о протоколах безопасности по всем указанным функциям. В политике конфиденциальности должны быть перечислены все сторонние приложения, которые имеют доступ к персональным данным.
	Как реализовать эту рекомендацию?	
	□ Включить в соглашения об обмене данными четкие положения о прекращении действия соглашения. □ Убедиться, что данные, полученные от негосударственного сектора, подпадают под действие законов о защите данных и должной осмотрительности, в том числе, когда они приобретаются или передаются добровольно. □ Разработать и опубликовать условия предоставления услуг, политики конфиденциальности и информацию о том, какие данные будут использоваться, кем и каким образом. □ Политика конфиденциальности должна быть понятной и всеобъемлющей, а также содержать обоснование использования любых сторонних приложений.	
Применимые инструменты реализации		
● Шаблон уведомления о конфиденциальности для приложения по отслеживанию контактов		

Функциональная Избыточность и Непредвиденные Последствия		
Тренд 4		
Отсутствие общественного доверия и осведомленности влияет на использование приложений по отслеживанию контактов	**Оценка**	Во всех рассматриваемых странах внедрению приложений по отслеживанию контактов препятствовали либо отсутствие общественного доверия, либо низкая осведомленность населения. Отчасти это было вызвано недостаточной агитацией по поводу приложений, а также отсутствием целенаправленных и адресных информационных сообщений со стороны правительства, что привело общественность в замешательство относительно отдельных приложений. Кроме того, в отношении некоторых приложений появились опасения, связанные со слежкой и неприкосновенностью частной жизни.
	Рекомендация	Органы государственной власти должны предпринимать целенаправленные и адресные усилия по информированию общественности, обеспечивая доступ к точной и своевременной информации о Covid-19. Предоставляемый контент должен носить научный и профессиональный характер, тогда он будет способствовать повышению осведомленности и знаний среди населения и, следовательно, улучшению его реакции на принимаемые меры и вводимые ограничения. Органы государственной власти должны обеспечить регулярное проведение прозрачных, демократических и научных консультаций с представителями гражданского общества.
	Как реализовать эту рекомендацию?	

	□ Приложения по отслеживанию контактов могут внести значимый вклад в эффективность общественного здравоохранения только в том случае, если они будут широко использоваться населением, что требует доверия. Использование передовых мировых стандартов (таких как минимизация данных и узкоцелевое предназначение приложений) и общие усилия по предотвращению функциональной избыточности являются ключевыми элементами выстраивания и поддержания общественного доверия. Далее по тексту настоящего Набора инструментов в разделе "Инструменты реализации" приведен шаблон спецификации требований к программному обеспечению.

Функциональная Избыточность и Непредвиденные Последствия		
Тренд 5		
Дискриминация в отношении социально незащищенных групп	**Оценка**	В некоторых из рассматриваемых стран были разработаны приложения, позволяющие гражданам сообщать государственным органам о нарушителях режима изоляции, используя с этой целью функции для уведомления властей о массовых скоплениях людей и приезжих из-за рубежа в определенном районе. Однако это может иметь серьезные последствия для социально отчуждённых групп, когда членов общества просят осуществлять наблюдение от имени государства без обязательств по обеспечению равенства, которые государства обычно должны соблюдать. Таким образом, пользователи получают возможность несправедливо подвергать преследованию определенных лиц или даже целые группы. В то время как меры, направленные на противодействие Covid-19, в частности, национальный карантин и строгий пограничный контроль, влияют на целые группы населения, мигранты и беженцы подвергаются повышенному риску изоляции или дискриминации. Обеспечение защиты уязвимых сообществ от указанных рисков зачастую непросто организовать, как это видно на примере ряда стран. Многие люди страдают от ограничений на передвижение, особенно когда разрешение на поездку можно получить только через цифровые платформы. Некоторые даже испытывают трудности с поиском жилья в разгар национального карантина, как это было в отдельных странах.

		Covid-19 также обострил проблемы, с которыми сталкиваются сельские жители и работники сектора неформальной экономики, такие как, например, недостаточное водоснабжение и перенаселенность. И все это в дополнение к спорному использованию карантинных лагерей, где мигранты содержались в изоляции в течение нескольких недель без тестирования на Covid-19 и были лишены возможности самоизоляции.
	Рекомендация	Органы государственной власти должны обеспечить равномерное применение санитарных мероприятий по всей стране. Органы государственной власти должны гарантировать предоставление услуг уязвимым группам населения (таким как мигранты и беженцы), чтобы они могли пережить трудности, связанные с пандемией. Такие услуги включают доступ к здравоохранению, материальной помощи и образованию. Органы государственной власти должны гарантировать всем людям отсутствие наказания или лишения доступа к какой-либо услуге, государственной или частной, вследствие отказа от использования приложения Covid-19. Предлагаемые меры в области общественного здравоохранения должны учитывать анализ возможных последствий их принятия для уязвимых групп населения.
	Как реализовать эту рекомендацию?	
	□ Не поощрять и не требовать от людей сообщать о «нарушителях» мер противодействия коронавирусной инфекции, поскольку эта роль является прерогативой органов государственной власти.	

	□ Обеспечить равномерное применение мер по охране здоровья населения по всей стране и независимый надзор за их применением, а также механизмами возмещения ущерба. □ Обеспечить включение мигрантов и беженцев в политику общественного здравоохранения, социального обеспечения и другие системы оказания поддержки. □ Обеспечить наличие бумажных (нецифровых) альтернатив приложениям по отслеживанию контактов для людей, не имеющих смартфона или не желающих пользоваться приложениями. □ Обеспечить продолжение рассмотрения ходатайств о предоставлении убежища, чистого и безопасного жилья, в том числе новые решения, такие как проживание в гостиницах (которые в противном случае пустовали бы из-за кризиса). □ Органы государственной власти должны проводить оценку воздействия на права человека, которая также должна включать потенциальное воздействие на различные уязвимые группы населения.

Функциональная Избыточность и Непредвиденные Последствия		
Тренд 6		
Подавление протестов	**Оценка**	В ряде рассматриваемых стран вспыхнули протесты в ответ на недостаточную помощь со стороны национальных и региональных властей в решении проблем, вызванных закрытием магазинов и другими мерами противодействия Covid-19. В некоторых случаях это привело к тому, что правоохранительные органы применяли непропорционально большую силу для подавления протестов, от чего пострадали дети, больные и пожилые люди. Из другого анализа по странам стало очевидно, что протесты усилились в ответ на якобы неправильное управление экономическим кризисом со стороны правительства во время пандемии. Протесты также подпитывались отсутствием государственной поддержки во время национального карантина, что усугубляло переживаемый многими экономический спад. Демонстрации привели к жертвам во время столкновений с силовыми структурами, когда власти пытались подавить протесты, в том числе во время общенационального карантина.
	Рекомендация	Правительства не должны использовать политику противодействия Covid-19 для запугивания и подавления политических диссидентов, а также для наказания диссидентов, находящихся в заключении.
	Как реализовать эту рекомендацию?	

	□ Политика в области общественного здравоохранения и законодательные акты должны основываться на фактических данных и иметь четко определенные цели, направленные на борьбу с распространением Covid-19 и позволяющие в максимально возможной степени продолжать социальную и экономическую деятельность, а также в полной мере пользоваться основными правами в указанных пределах. □ Следует создавать (в том случае, если их еще нет) и развивать механизмы возмещения ущерба в случаях нарушения основополагающих прав во время пандемии. При наличии указанных механизмов необходимо их реализовать самым эффективным образом.

Функциональная Избыточность и Непредвиденные Последствия		
Тренд 7		
Технологические меры противодействия Covid-19 усугубили цифровое неравенство	**Оценка**	Неравенство в отношении доступа к интернету и мобильным технологиям влияет на возможность доступа людей к общественным функциям во время пандемии. Это критически важный вопрос, поскольку неравный доступ к указанным ресурсам может усугубить существующее неравенство и вызвать проблемы этического характера. Кроме того, при предоставлении услуг социального обеспечения преимущественно через онлайн-платформы, уязвимые сообщества, многие из которых не имеют адекватного доступа к интернету и большого числа мобильных устройств, могут вообще лишиться доступа к социально значимым услугам. Однако даже при наличии доступа к онлайн-платформам их реализация может иметь негативные последствия, которые выходят за рамки потенциального вреда для уязвимых сообществ. Например, некоторые приложения по отслеживанию контактов были доступны только на английском языке, хотя их пользователи говорят на местных языках.

	Рекомендация	Необходимо разработать и сделать доступными цифровые материалы. Эти материалы должны быть понятными и адекватными, сопровождаться обучением и инструментами, разъясняющими, как использовать соответствующее приложение, а также освещающими основные вопросы конфиденциальности данных. Необходимо организовать обучение цифровой грамотности для сотрудников государственных органов, работников системы здравоохранения и пользователей приложений. Органы государственной власти должны разработать альтернативные, нецифровые способы подачи заявок на перемещение и регистрацию вакцинации.
	Как реализовать эту рекомендацию?	
	□ Обеспечить наличие бумажных (и нецифровых) альтернатив для всех мер и инициатив по противодействию распространению Covid-19, включая, помимо прочего, отслеживание контактов, приложения по отслеживанию контактов и доступ к социальному обеспечению. □ Решить проблему дистанционного образования, которое ставит в невыгодное положение детей, находящихся в экономически неблагоприятных условиях. □ Обеспечить проведение политики и финансирования, нацеленных на предотвращение возникновения и усугубления цифрового неравенства среди детей.	

Эффективность в здравоохранении		
Тренд 1		
Недостаточная опора на фактические данные при выработке решений	**Оценка**	Порядок и ответные меры по отработке чрезвычайного положения должны иметь весомое обоснование для обеспечения их эффективности. Таким образом, в контексте пандемии Covid-19, все санитарно-гигиенические меры должны быть адаптированы к особенностям страны или региона и соответствовать актуальным научным данным. Правительства с переменным успехом привлекали органы общественного здравоохранения и других соответствующих экспертов к процессу принятия решений о выработке мер по предотвращению распространения Covid-19.
	Рекомендация	В случаях, когда технологические решения являются частью мер по предотвращению распространения инфекции, правительства должны убедиться в наличии соответствующей критический инфраструктуры, способной обеспечить максимально возможную эффективность таких мер. Интернет-инфраструктура, особенно в контексте мобильных приложений или других веб-сервисов, должна быть разработана таким образом, чтобы доступ к сети интернет был в достаточной мере распределен среди населения, и обеспечивал при этом стабильную подключение к сервисам.

		Технологические меры реагирования на чрезвычайную ситуацию в области здравоохранения должны быть основаны на соответствующих научных данных для обеспечения их эффективности. Органы здравоохранения и другие организации, объединяющие экспертов в этой области, должны быть на должном уровне вовлечены в процесс выработки решений в достаточной мере, чтобы директивные органы могли обеспечить и обосновать, что выработанные ими санитарно-гигиенические меры основаны на актуальных научных данных и адекватны сложившейся обстановке чрезвычайной ситуации.
	Как реализовать эту рекомендацию?	
	□ Центральные органы власти должны оценить текущее положение дел по вопросу распределения критической интернет-инфраструктуры в своих странах с тем, чтобы выявить требующие дополнительного развития области. □ В выявленных областях, нуждающихся в развитии, должны быть произведены инвестиции в критическую интернет-инфраструктуру. Это могут быть такие направления как субсидированный мобильный трафик, бесплатные точки доступа Wi-Fi и даже программы цифровой грамотности. □ Непосредственно перед внедрением, директивные и законодательные органы должны через консультации с экспертным сообществом удостовериться, что выбранные технологии внесут существенный вклад в борьбу с Covid-19 и не несут большого сопутствующего вреда для того, чтобы оправдать их применение. Результаты подобных дебатов могут быть представлены в форме рекомендаций и переданы упомянутой ниже полномочной комиссии. В любом случае, эти рекомендации должны быть доступны общественности через открытые источники.	

	□ Учредить комиссию, уполномоченную на принятие решений, состоящую из: независимых представителей сектора здравоохранения (эпидемиологов), технических специалистов, представителей директивных органов и органов по надзору за соблюдением законодательства о защите персональных данных. Решения комиссии должны подлежать регулированию через механизм сдержек и противовесов.

Эффективность в здравоохранении		
Тренд 2		
Недостаточная общественная осведомленность в части научных достижений, на которых основаны меры противодействия Covid-19	**Оценка**	Инфекция Covid-19 стремительно распространилась по всему миру и явилась для большинства людей неизвестной ранее опасностью. И правительства, и отдельные граждане были вынуждены быстро учиться, а также – особенно на ранних этапах – принимать решения в условиях ограниченной информации. Во многих странах также наблюдался рост популярности теорий заговора, касающихся этой болезни. Все большее число фактов указывает на то, что хорошо спланированные кампании по информированию населения существенно влияют на соблюдение гражданами социальной дистанции, карантинных мер и также рекомендаций по вакцинированию. В ряде стран подобные информационные кампании внесли существенный вклад в такие показатели как активное выполнение санитарно-гигиенических мер, локальное производство защитных масок в тех районах, где они не были доступны, а также готовность к вакцинации.
	Рекомендация	Создание “коалиций сторонников” с широким вовлечением общественных организаций. Информационно-просветительские кампании, как онлайн, так и оффлайн, могут улучшить готовность населения выполнять санитарно-гигиенические требования и предотвратить утрату доверия. Необходимо принимать во внимание демографические особенности, особенно среди обособленных социальных групп, работая в таких сообществах с имеющими высокий уровень доверия группами лиц.

	Как реализовать эту рекомендацию?
	□ Партнерские программы общинного уровня могут быть эффективным средством повышения уровня осведомленности среди обособленных социальных групп.

Эффективность в здравоохранении		
Тренд 3		
Неэффективное проведение государственных закупок в рамках мер по противодействию Covid-19	**Оценка**	В некоторых правовых системах существуют положения об ускоренных процедурах закупок, позволяющих государству быстро закупить необходимые в чрезвычайной ситуации ресурсы в целях организации эффективного и быстрого отклика. При этом, в случаях, когда всеохватывающие положения об ускоренных государственных закупках не утверждены или не исполняются, может возникнуть ряд проблем, включая нехватку необходимого оборудования.
	Рекомендация	Наличие регулярных, а не временных или специальных регламентов публичных закупок во время чрезвычайных ситуаций обеспечит более высокую эффективность процесса государственных закупок товаров и услуг. В качестве дополнительной меры можно использовать заблаговременное размещение контрактов на приобретение товаров

		и услуг для обеспечения их быстрой доступности в случае возникновения упомянутой чрезвычайной ситуации.
	Как реализовать эту рекомендацию?	
	□ Внести на рассмотрение законопроект о государственных закупках, отражающий ключевые положения типового закона ЮНСИТРАЛ о публичных закупках или иного аналогичного международного стандарта. Особое внимание следует уделить пунктам, касающимся закупок в случаях крайней срочности. Такие пункты могут включать, к примеру, следующее: ● Закупки из одного источника допустимы только в том случае, когда в этом есть крайне срочная потребность вследствие чрезвычайного события и использование любого другого метода закупок было бы практически нецелесообразным с учетом того времени, которое необходимо для использования таких методов (аналогично Статье 30.5(b) ЮНСИТРАЛ). ● С поставщиком проводятся переговоры с целью формирования предложения или ценовой котировки, за исключением случаев, когда такие переговоры не могут быть практически проведены в обстоятельствах соответствующих закупок (аналогично Статье 52 ЮНСИТРАЛ). ● Товары и услуги могут быть приобретены у определенных поставщиков в срочных случаях в соответствии с соглашениями, заключенными между государством и такими поставщиками до возникновения чрезвычайной ситуации, которая является причиной такой срочности.	

Функциональная Избыточность и Непредвиденные Последствия		
Тренд 1		
Отсутствие законодательной базы необходимой для развертывания и применения приложений Covid-19	**Оценка**	В отдельных странах исследования приложения и санитарно-гигиенические меры, предназначенные для борьбы с распространением Covid-19, часто развертывались на фоне отсутствия законодательной базы, регламентирующей их применение и разрешающей центральным органам власти создание и развертывание приложений Covid-19. В ряде случаев отсутствовало законодательство в области обработки персональных данных, необходимое для функционирования приложений Covid-19. Из-за этих пробелов в законодательстве, функциональная избыточность становится более вероятным риском, что может означать возможность использования центральными органами власти этих мер и персональных данных в целях, отличных от борьбы с распространением Covid-19.
	Рекомендация	Обеспечить внедрение всеохватывающего законодательства, на котором будет базироваться выработка мер реагирования на экстренные ситуации. Внести в конституцию страны или ее правовую систему положение о чрезвычайной ситуации, которое, на ограниченное время, стало бы основанием для изменения полномочий ряда государственных органов во время чрезвычайной ситуации для обеспечения надзора и гарантий защиты прав личности.
	Как реализовать эту рекомендацию?	

	□ Предоставить на рассмотрение законопроект, вносящий в законодательство следующие положения: ● Органы исполнительной власти или правительства имеют право объявить чрезвычайное положение, с условием, что разрешение на такие действия предварительно одобрены центральным законодательным органом. ● Органы законодательной и судебной власти осуществляют надзорные функции во время чрезвычайного положения. ● Правительство может утверждать меры реагирования в связи с объявленным чрезвычайным положением только в том случае, когда содержание и масштаб таких мер реагирования четко определены законодательством. ● Меры реагирования, введенные в связи с чрезвычайным положением, не должны противоречить существующему законодательству, включая, но не ограничиваясь законами о защите данных. ● Правительство должно обеспечить, что умаление или ограничение любых прав личности, которые закреплены в правовой системе или конституции, отвечает критерию соразмерности. ● Меры реагирования, введенные в связи с чрезвычайным положением, подлежат последующей проверке и утверждению со стороны органов законодательной власти. ● Чрезвычайное положение и меры реагирования, введенные в связи с чрезвычайным положением, должны сопровождаться строгим ограничением по времени, любое продление сроков действия должно быть предварительно одобрено органами законодательной власти.

<table>
<tr><th colspan="3">Функциональная Избыточность и Непредвиденные Последствия</th></tr>
<tr><td colspan="3">Тренд 2</td></tr>
<tr><td rowspan="3">Ограниченный или неравный доступ к общественным ресурсам</td><td>Оценка</td><td>Иногда во время чрезвычайного положения правительства вводят в действие меры, которые могут привести к дискриминации отдельных групп граждан. В контексте пандемии Covid-19 отдельные меры были объявлены обязательными, несмотря на то, что фактически отсутствовали достаточные ресурсы и меры поддержки для обеспечения возможности их исполнения. К примеру, в ряде стран было объявлено требование о необходимости вакцинации от Covid-19 для получения возможности посещения общественных мест или путешествий, несмотря на ограниченную доступность вакцин или тот факт, что значительная доля населения не была вакцинирована на момент введения требования.</td></tr>
<tr><td>Рекомендация</td><td>Правительства должны обеспечить условия, при которых обязательные санитарно-гигиенические меры, введенные во время чрезвычайного положения, связанного с риском для общественного здоровья, подкреплены необходимыми ресурсами и средствами, чтобы граждане имели возможность исполнять соответствующие меры и избежать несправедливой изоляции от общества.</td></tr>
<tr><td colspan="2">Как реализовать эту рекомендацию?</td></tr>
<tr><td></td><td colspan="2">□ Обеспечить широкую доступность для населения мер, требуемых для доступа к общественной жизни, в том числе вакцинация, тесты и бумажные альтернативы приложениям.</td></tr>
</table>

	□ Центры вакцинации и тестирования должны быть доступны как городских, так и в сельских районах; бумажные или нецифровые альтернативы приложениям должны быть легкодоступны.

2. Рекомендации для разработчиков приложений, операторов информационных систем и осуществляющих приемку бюджетных организаций

Чего общественность может ожидать от заинтересованных сторон, участвующих в реализации мер противодействия пандемии, и почему?

Для широкой общественности важно понимание, что разработчики и операторы информационных систем, а также бюджетные организации, задействованные в приемке приложений Covid-19, могут предпринять ряд действий, направленных на обеспечение эффективной и устойчивой эксплуатации данных приложений. Эти действия выражаются в проектных и программных решениях, мерах защиты и процедурах, которые в комплексе предназначены для обеспечения доверия и успешного использования приложений Covid-19 как составляющей части более широкой санитарно-эпидемиологической стратегии.

На практике технические особенности и архитектура приложений Covid-19 влияют на сбор и использование персональных данных граждан, а также на реализацию ими основополагающих прав, включая право на неприкосновенность частной жизни.

В частности, открытие кода приложения для публичного доступа укрепляет общественное доверие к нему. Применение концепции "проектируемая конфиденциальность" может помочь предотвратить функциональную избыточность и другие непреднамеренные последствия, предотвратить утрату доверия и другие негативные последствия внедрения приложения. Сюда также входит ограничение на использование необязательных данных, в том числе локационных данных, применению которых обычно есть альтернативы. Обработка персональных данных должна быть четко регламентирована, особое внимание уделено целям обработки, степени чувствительности данных, порядку хранения, обеспечения сохранности, и ограничениям на передачу. Любая форма передачи данных, особенно представителям частного сектора, должна служить четко определенной цели в рамках санитарно-эпидемиологической стратегии, за возможным исключением в виде данных научных исследований, особенно тех, которые предназначены для выработки политики общественного здравоохранения в будущем.

Приложение также должно быть спроектировано с учетом задела на будущее в части предупреждения потенциальных возможностей использования в мошеннических целях, в пределах ранее перечисленных правовых ограничительных принципов. Функционирование приложения может быть гарантировано только в том случае, если произошедшие случаи мошенничества могут быть эффективно и прозрачно отработаны.

Эффективность в здравоохранении		
Тренд 1		
Не все приложения имеют открытый исходный код	**Оценка**	Во всех проанализированных приложениях есть недостатки в части прозрачности, при этом между ними есть существенные различия. Только три приложения используют открытый для изучения код. Большая часть использует т.н. "маскировку кода", процесс рефлексии и другие затрудняющие анализ подходы, которые делают сложным или даже невозможным надежное подтверждение совершения программой определенных действий. Такие меры негативно отражаются на уровне доверия и противоречат международным рекомендациям по прозрачности и проектированию систем, работающих с персональными данными.
	Рекомендация	Опубликовать исходный код существующих приложений для Covid-19 на всех платформах. Открытие серверного кода в свободном доступе для общественного аудита позволяет наладить коллаборацию, проверить код на наличие уязвимостей и перейти на использование системы независимой экспертизы.
	Как реализовать эту рекомендацию?	

	□ Опубликовать исходный код на GitHub или другом аналогичном сайте или платформе □ Не использовать методы обфускации для сокрытия или искажения исходного кода, затрудняющие процесс независимого анализа кода.

Функциональная Избыточность и Непредвиденные Последствия		
Тренд 1		
Развертывание технологических решений в сотрудничестве с предприятиями частного сектора	**Оценка**	Некоторые партнерские программы представляют собой соглашения о совместном использовании данных. Другие партнерские программы были связаны с частными компаниями, помогающими государственным органам проводить операции по негласному наблюдению. Большой недостаток таких партнерских программ – это отсутствие соответствующего законодательного регулирования. Более того, во всех странах исследования отсутствовало полноценное законодательство в области защиты данных, что подвергает еще большему сомнению легитимность таких государственно-частных партнерств и создает предпосылки для функциональной избыточности и злоупотреблении властными полномочиями.
	Рекомендация	Использовать прозрачный механизм совместного использования данных между различными государственными органами и организациями частного сектора.

	Как реализовать эту рекомендацию?
	□ Свериться с соответствующей спецификацией требований к программному обеспечению с тем, чтобы определить необходимость совместного использования данных для функционирования приложения или системы, или одной из их функций. □ Сформировать карты движения потоков данных и обеспечить протоколирование операций по обработке данных с целью документирования данных, которые были переданы государственным органам, а также целей такой передачи. В разделе "Инструменты реализации" для примера того, что должен содержать такой документ приведен соответствующий шаблон. □ Провести консультационную работу с экспертами в области права с целью составления юридических формулировок, касающихся передачи данных государственным органам, целей такой передачи и других соответствующих обязательств, применимых к ней. Эти формулировки должны быть включены в любой договор на оказание услуг между разработчиком и правительством.
Применимые инструменты реализации	
● Шаблон спецификации требований к программному обеспечению ● Шаблон карты потока персональных данных приложения по отслеживанию паспортов иммунизации	

<table>
<tr><th colspan="3">Функциональная Избыточность и Непредвиденные Последствия</th></tr>
<tr><td colspan="3">Тренд 2</td></tr>
<tr><td rowspan="3">Большинство стран приняли решение выбрать централизованную модель при разработке программ по отслеживанию контактов</td><td>Оценка</td><td>Считается, что централизованные системы меньше отвечают требованиям концепции "проектируемая конфиденциальность", чем децентрализованные. В централизованной модели большая часть необходимых вычислений производится на центральном сервере, оператором которого является полномочный орган государственной власти, что делает персональные данные легкодоступными для этого органа. В децентрализованной модели, напротив, большая часть вычислений производится на устройстве пользователя, наиболее чувствительная информация хранится локально, другим устройствам и центральным серверам передают только псевдоанонимизированные данные. Именно такую модель используют страны, выбравшие интерфейс GAEN API.</td></tr>
<tr><td>Рекомендация</td><td>Разработку приложений рекомендуется вести в рамках концепции "проектируемая конфиденциальность".</td></tr>
<tr><td colspan="2">Как реализовать эту рекомендацию?</td></tr>
<tr><td colspan="3">□ Разработать спецификацию требований к программному обеспечению для процесса разработки приложения, в которой изложены предлагаемые функции приложения Covid-19 в соответствие с ключевыми принципами сохранения конфиденциальности и юридическими требованиями. В разделе "Инструменты реализации" приведен соответствующий шаблон.</td></tr>
</table>

	□ Провести консультационную работу с независимыми сторонними экспертами для оценки приложений Covid-19 на предмет рисков, связанных с защитой данных и конфиденциальностью в процессе их разработки для того, чтобы обеспечить корректную интерпретацию и реализацию принципов защиты данных и приватности на каждом этапе цикла проектирования до начала развертывания приложения.
Применимые инструменты реализации	
● Шаблон спецификации требований к программному обеспечению	

Функциональная Избыточность и Непредвиденные Последствия		
Тренд 3		
Широкое использование данных о местоположении	**Оценка**	Сбор геоданных позволяет центральным органам власти отслеживать местоположение пользователей и осуществлять другие формы негласного наблюдения, выходящие за рамки необходимости, связанной с охраной общественного здоровья. Особенную озабоченность вызывает возможность использования данных о местоположении для выявления "привычек пользователей, их адресов проживания и работы, и даже религиозных верований (напр., мест богослужения).”

	Рекомендация	Минимизировать количество собираемых данных до строго необходимых объемов, особенно в части персональных и идентифицируемых данных; сюда входит исключение необходимости сбора данных о местоположении GPS. Убрать запросы на доступ к данным о местоположении из всех приложений по отслеживанию контактов в целях обеспечения требований приватности. Предоставить простую и легкодоступную возможность удаления аккаунта и данных из приложения, а также с сервера.
	Как реализовать эту рекомендацию?	
	□ Проводить регулярный анализ кода в процессе его написания от высокоуровневого проекта до отдельных строк. □ Привлекать экспертов или специалистов по защите данных и приватности для обеспечения соответствия функционирования приложения спецификации требований к ПО, содержащей соответствующие юридические требования и принципы.	

Функциональная Избыточность и Непредвиденные Последствия		
Тренд 4		
Частое использование инструментов отслеживания и аналитики	**Оценка**	В странах исследования принцип проектируемой конфиденциальности не был полностью реализован в отношении используемых пакетов разработки ПО (SDK). В частности, использование библиотеки Google Firebase, а также других SDK не было явно описано в соответствующих политиках конфиденциальности. В этих случаях невозможно в полной мере определить как именно использовалась библиотека Google Firebase, в частности, ограничивалось ли её применение анализом числа установок или же отслеживался более широкий круг параметров, потенциально нарушающий принципы приватности.
	Рекомендация	Предоставить ясную информацию о типах собираемых данных и целях их сбора, информации о том, где и как хранятся эти данные, каким организациям и в каких целях эти данные могут быть переданы, а также о протоколах безопасности, используемых при осуществлении всех этих функций. Опубликовать более подробные тексты политики конфиденциальности (на всех используемых в регионе языках) и прямо указать в них все третьи стороны, имеющие доступ к данным.
	Как реализовать эту рекомендацию?	

	□ Провести процедуры аудита поставщика в отношении разработчиков SDK и других библиотек, используемых в приложении Covid-19. Такой аудит должен включать анализ политики приватности и другой значимой документации в области защиты данных, а также инспекцию стороннего кода, импортируемого в рабочую среду для разработки приложения.

Эффективность в здравоохранении		
Тренд 1		
Мошеннические действия с целью получения сертификатов Covid-19	**Оценка**	Частично вследствие дезинформации и связанных с Covid-19 теорий заговора, имеется ряд случаев, когда граждане пытались получить поддельные QR коды для того, чтобы посещать общественные места и путешествовать. В некоторых странах число случаев подобного мошенничества исчислялось десятками тысяч.
	Рекомендация	Предупреждать попытки мошеннических действий и обеспечить надлежащую проверку всех вовлеченных сторон, включая организации частного сектора. В рамках принципов проектируемой конфиденциальности, предусмотреть возможность удаления сертификатов, полученных ненадлежащим образом, и обеспечить прозрачную интеграцию этого процесса в положении о конфиденциальности.
	Как реализовать эту рекомендацию?	

	□ Провести проверочные испытания с целью обеспечения функционирования системы согласно требованиям. В эту процедуру должны входить модульное тестирование (охватывающее отдельные функции и системные компоненты), комплексные испытания (охватывающие взаимодействие между группами компонентов), системные испытания (охватывающие завершенные блоки единой системы), и приемочные испытания (предоставление системы отдельным пользователям, т.е. альфа- и бета-тестирование).

Функциональная Избыточность и Непредвиденные Последствия		
Тренд 1		
Неприверженность концепции проектируемой конфиденциальности в приложениях Covid-19	**Оценка**	Приложения Covid отличаются разным уровнем реализации концепции проектируемой конфиденциальности. Если эта концепция не реализована, пользователям может быть нанесен непропорциональный ущерб. Подобные недоработки могут зачастую приводить к тому, что разработчики, а также государственные органы, пользующиеся их услугами, оказываются не в состоянии защитить приватность, а пользователи не могут реализовать права на защиту данных должным образом. Некоторые приложения используют SDK, которые обрабатывают данные с целями, отличными от основного назначения приложения (общественное здравоохранение) или передают данные третьим лицам. В дополнение к этому, большинство разработчиков не раскрывают используемые ими при разработке приложений сторонние SDK и программные библиотеки, а также не публикуют или иным образом скрывают исходный код. Также, большинство приложений Covid-19 были развернуты без заблаговременного проведения аудита уровня защиты данных и оценки рисков приватности. При этом, некоторые страны приложили усилия к тому, чтобы обеспечить методическую помощь общественным заведениям, от которых требовался сбор персональных данных в целях отслеживания контактов.
	Рекомендация	Использовать только те SDK, которые осуществляют обработку исключительно необходимой для задач приложения персональной информации (т.е. отслеживания контактов или вывода на дисплей информации медицинского характера).

		Подготовить уведомления о конфиденциальности, информирующие пользователей приложения в краткой и доступной форме о том, как именно осуществляется сбор и обработка их персональных данных, и в удобной для пользователей форме демонстрировать такие уведомления. Сделать исходный код приложения открытым для обеспечения возможности независимой верификации функций приложения и порядка обработки им персональных данных. В случаях, когда обработка персональных данных осуществляется силами общественного заведения (к примеру, в случаях, когда применяется и цифровое и ручное отслеживание контактов), предоставить методическую помощь в вопросах обработки таких данных с целью обеспечения высоких уровней ответственности и защиты данных. Провести оценку уровня защиты персональных данных и оценку последствий с точки зрения сохранения конфиденциальности перед развертыванием приложения для выявления потенциальных рисков защиты данных или рисков, связанных с конфиденциальностью, а также выработать адекватные меры снижения этих рисков.
	Как реализовать эту рекомендацию?	
	□ Привлекать независимых сторонних экспертов в роли консультантов для оценки уровня рисков, связанных с защитой персональных данных, и рисков приватности приложений Covid-19 в процессе их разработки для обеспечения корректности применения принципов защиты данных и приватности на каждом этапе цикла разработки вплоть до развертывания приложения.	

	Разработать спецификацию требований к программному обеспечению для процесса разработки приложения, описывающую требуемые функции приложения Covid-19 в соответствии с принципами приватности и юридическими требованиями. В разделе "Инструменты реализации" для примера того, что должен содержать такой документ приведен соответствующий шаблон. □ Провести процедуры аудита поставщика в отношении третьих сторон, предоставляющих SDK и другие библиотеки, используемые в приложении Covid-19. Такой аудит должен включать анализ текста политики приватности и другой значимой документации в области защиты данных, а также инспекцию стороннего кода, импортируемого в рабочую среду для разработки приложения. □ Подготовить развернутое уведомление о конфиденциальности, а также его краткую версию, демонстрируемую пользователям при первом запуске приложения и доступную впоследствии. В разделе "Инструменты реализации" приведён соответствующий шаблон. □ Опубликовать исходный код на GitHub или другом аналогичном сайте или платформе для ПО с открытым кодом. □ Не использовать методы обфускации для скрытия или искажения кода, затрудняющие независимый анализ кода. □ Подготовить методические пособия для операторов общественных заведений, включающие информацию о том (1) какие данные и с какими целями подлежат сбору, (2) как именно должен осуществляться сбор и хранение таких данных, (3) какие существуют требования по сохранению конфиденциальности этих данных, и (4) что данные могут быть переданы только специально указанным третьим лицам, связанным с процессом сбора таких данных. □ В разделе "Инструменты реализации" приведён соответствующий шаблон, который можно использовать как отправную точку для подготовки оценки уровня рисков, связанных с

	защитой персональных данных, и оценки последствий с точки зрения сохранения конфиденциальности для их проведения в ходе процесса разработки приложения.
Применимые инструменты реализации	
● Шаблон спецификации требований к программному обеспечению ● Шаблон уведомления о конфиденциальности для приложения по отслеживанию контактов ● Шаблон оценки воздействия на защиту данных/ конфиденциальность	

Функциональная Избыточность и Непредвиденные Последствия		
Тренд 2		
Широкое распространение частно-государственных партнерств и отсутствие прозрачности	**Оценка**	Правительства часто стремятся использовать свои взаимоотношения с организациями частного сектора для достижения политических целей. Ситуация вокруг Covid-19 не стала исключением: многие правительства стремятся использовать систему Google/Apple Exposure Notification для разработки на ее основе собственных приложений по отслеживанию контактов. Некоторые страны обращаются к телекоммуникационным операторам для получения данных для создания карт частотности и отслеживания параметров распространения вируса. Правительства также используют системы видеонаблюдения для отслеживания выполнения требований карантинизации, тем самым расширяя аппарат государственной слежки. Часто такие партнерские отношения держатся в тайне или, в контексте Covid-19, используют предлог чрезвычайного положения для обхода обычных регуляторных рамок, существующих для защиты прав.

	Рекомендация	Для всех приложений, разработанных в рамках частно-государственного партнерства, открыть для публичного доступа условия партнерства.
	Как реализовать эту рекомендацию?	
	□ Государство должно обеспечить прозрачность частно-государственных партнерств (например посредством удовлетворения запросов о предоставлении публичной информации).	

Инструменты реализации

Ниже приведены шаблоны, а также примеры из передовой практики, способствующие реализации некоторых рекомендаций, представленных в наборе инструментов для приложений Covid-19.

Реализация концепции проектируемой конфиденциальности для приложений по отслеживанию контактов

В данном примере представлена модель приложения по отслеживанию контактов с повышенной конфиденциальностью, генерирующего свои собственные QR-коды, которые используются физическими лицами (с их согласия) для регистрации при входе в заведения, зарегистрированные в этом приложении («Зарегистрированные заведения») и при выходе из них.

Эти приложения должны разрабатываться с единственной целью: упростить регистрацию входа в зарегистрированные заведения и выхода из них при условии защиты конфиденциальности и персональных данных, это означает, что:

a. Приложение обрабатывает минимально возможный объем персональных данных;
b. Персональные данные максимально зашифрованы и могут быть расшифрованы органом здравоохранения только в случае выявления случая заболевания Covid-19;
c. Орган общественного здравоохранения получает только те данные, которые необходимы для отслеживания физических лиц, присутствовавших в конкретном месте и в конкретное время, для которых был выявлен риск передачи Covid -19;
d. Все данные о входе-выходе удаляются, как только они утрачивают актуальность для целей отслеживания контактов, а именно через 14 дней.

Доступ к данным и передача данных

- Разработчик или оператор приложения не должен иметь доступ к персональным данным, полученным от физического лица, обрабатываемым зарегистрированными учреждениями или переданным в орган здравоохранения.
- Заведения, использующие приложение для регистрации входа и выхода физических лиц, имеют строго ограниченный доступ к личным данным, которые видны только на момент входа для облегчения проверки личности в случае необходимости. Только уполномоченный персонал заведения имеет доступ к этим данным.
- Орган общественного здравоохранения имеет право получать данные о лицах, посетивших зарегистрированное заведение одновременно с человеком с диагнозом Covid-19 (в целях установления с ними контакта).

Заявленная цель

Персональные данные могут обрабатываться в следующих целях:

a. Предоставление физическим лицам QR-кода.
b. Обеспечение заведения безопасными средствами сбора данных о присутствующих.
c. Предоставление органу общественного здравоохранения данных, необходимых для выявления и установления контакта с лицами, которые могли находиться в непосредственной близости от человека, у которого диагностирован Covid-19.

Обрабатываемые данные

1. О лицах, использующих приложение:

   a. Имя, фамилия и год рождения, используемые для целей идентификации и отслеживания контактов.

   b. Номер мобильного телефона, используемый для получения QR-кода приложения и, при необходимости, для связи с органом общественного здравоохранения.

   c. Отметки о входе в заведение и выходе из него на основе QR-кодов, хранящиеся на устройстве отдельных лиц и серверах приложения, расшифровываемые и используемые для целей отслеживания в случае раскрытия информации заведением по запросу органа общественного здравоохранения.

2. О зарегистрированных заведениях
    a. Электронная почта, имя пользователя, пароль владельца учетной записи, используемые для создания и управления учетной записью.

    b. Имя, электронная почта и номер телефона трех контактных лиц заведения, используемые органом общественного здравоохранения для передачи запросов на раскрытие информации в целях отслеживания контактов.

3. Органом общественного здравоохранения
    a. Имя, фамилия, год рождения и номер мобильного телефона лиц, присутствовавших в определенном месте в определенный период времени, с целью идентификации и установления контакта с этими людьми для предотвращения распространения Covid-19.

Хранение и удаление данных

1. Зарегистрированные физические лица и QR-коды:
    a. Персональные данные, предоставленные для целей регистрации и получения QR-кода, удаляются сразу после получения физическим лицом ссылки на QR-код.

b. QR-код, содержащий зашифрованные персональные данные о физическом лице, сохраняется в двух местах:
    i. На устройстве физического лица, чтобы обеспечить возможность сканирования заведениями.
    ii. На сервере разработчика или оператора приложения, чтобы пользователь имел возможность скачать изображение по ссылке в SMS.

c. Пользователи могут удалить свой QR-код или связь между собой и своим QR-кодом в любое время, при этом любые записи входа-выхода с этим QR-кодом будут сохраняться в течение 14 дней для целей отслеживания контактов.

d. Все QR-коды и средства их расшифровки будут удалены, когда орган общественного здравоохранения отменит законодательное требование к заведениям по сбору данных о входе-выходе.

2. Данные о заведениях и их посетителях:
    a. Персональные данные, относящиеся к заведению, будут храниться до тех пор, пока:

i. Заведение не деактивирует свою учетную запись (в этом случае данные о заведении и связанные с ними данные о входе-выходе будут храниться в течение 14 дней для отслеживания контактов перед их удалением),
ii. Управление здравоохранения не отменит законное требование к заведениям по сбору данных о входе и выходе, при этом все учетные записи будут удалены.

b. Данные зарегистрированных заведений о входе-выходе автоматически удаляются через 14 дней.

c. Данные, переданные органу общественного здравоохранения для отслеживания контактов, обрабатываются в соответствии с применимыми национальными нормативными актами, политикой и процедурами.

3. Данные SMS удаляются приложением, а службы, используемые приложением для отправки сообщений, удаляют данные со своих серверов сразу после их доставки.

Disclosure of data to the Public Health Authority

1. Individuals' data are encrypted in their QR code. The data are linked to the venues visited when they scanned their QR code. The Public Health Authority may only access and decrypt the data if it is necessary for contact tracing.

Раскрытие данных органу общественного здравоохранения

1. Данные физического лица зашифрованы в его QR-коде. Эти данные связаны с местами, которые посетил человек, когда сканировал свой QR-код. Орган здравоохранения может получить доступ к данным и расшифровать их только в том случае, если это необходимо для отслеживания контактов.

2. В случае, если лицо с диагнозом Covid-19 было отслежено до заведения, орган общественного здравоохранения может запросить у этого заведения раскрытие информации о лицах, присутствовавших там в то же время. Заведение может разрешить передачу данных о соответствующих лицах или запросить у органа здравоохранения дополнительную информацию, если это необходимо для подтверждения запроса.

3. Разрешение на раскрытие информации позволяет органу общественного здравоохранения получить доступ к данным только о соответствующих лицах: тех, кто присутствовал в данном месте в указанный период времени.

Информационная безопасность

1. Информационная безопасность достигается за счет сегрегации данных, надежного контроля доступа и шифрования. Функции информационной безопасности, архитектура и база кода подлежат проверке и верификации независимыми специалистами в области компьютерных технологий.

Файлы Cookie

1. Для облегчения процессов создания учетной записи и обеспечения безопасности данных на веб-сайте приложения используются строго необходимые куки-файлы:
    a. «csrftoken» используется для защиты сервиса от межсайтовой подделки запросов.
    b. «sessionid» используется для правильного отнесения сервером сеансов к аутентифицированным пользователям, имеющим доступ к информационной панели.

Шаблон спецификации требований к программному обеспечению

Спецификация требований к программному обеспечению — это документ, содержащий подробное описание всех требований, которым должно соответствовать разрабатываемое приложение или информационная система. Этот документ может включать как технические, так и юридические требования. Ниже приведен пример раздела спецификации требований к программному обеспечению, содержащий юридические требования, которым должно соответствовать приложение по отслеживанию контактов.

Идентификатор требования	REQ-31
Описание требования	Приложение должно использовать Google/Apple Exposure Notification Framework в качестве модели отслеживания контактов
Автор	[Имя]
Редакция	1.1
Дата публикации	[Дата]
Ключевые слова	Децентрализованное отслеживание контактов, минимизация данных
Юридическое требование	*Принцип ограничения сбора данных FIPPs* – сбор персональных данных должен быть ограничен, и любые такие данные при необходимости могут быть получены с использованием законных и надлежащих средств, с ведома или согласия субъекта данных.
Описание сценария Приложения, использующие GAEN, генерируют случайные идентификаторы (криптографические маркеры, называемые дистанционными идентификаторами), которые обновляются каждые 10-20 минут, чтобы отразить местоположение устройства. Когда пользователь вступает в тесный контакт с другим устройством с приложением, использующим систему GAEN, два устройства обмениваются информацией и записывают свои случайные идентификаторы через Bluetooth. Пользователи также вводят свои положительные результаты теста на Covid-19 в приложение, и список случайных идентификаторов, которые были зарегистрирован устройством за последние 14 дней, передается на центральный сервер, управляемый государственным органом. Затем мобильное устройство периодически сравнивает записанные им случайные идентификаторы с базой данных идентификаторов, связанных с положительным результатом теста на Covid-19. При обнаружении совпадения приложение уведомит пользователя о том, что он, возможно, подвергся заражению Covid-19, и посоветует следовать указаниям соответствующего	

государственного органа, например, сдать тест на Covid-19 или самоизолироваться на определенный период.

Исходные условия проектирования

Криптографические токены на устройстве меняются регулярно в соответствии с местоположением устройства.

На центральном сервере, находящемся под контролем государственного органа, хранятся только псевдонимные личные данные пользователей (криптографические случайные идентификаторы).

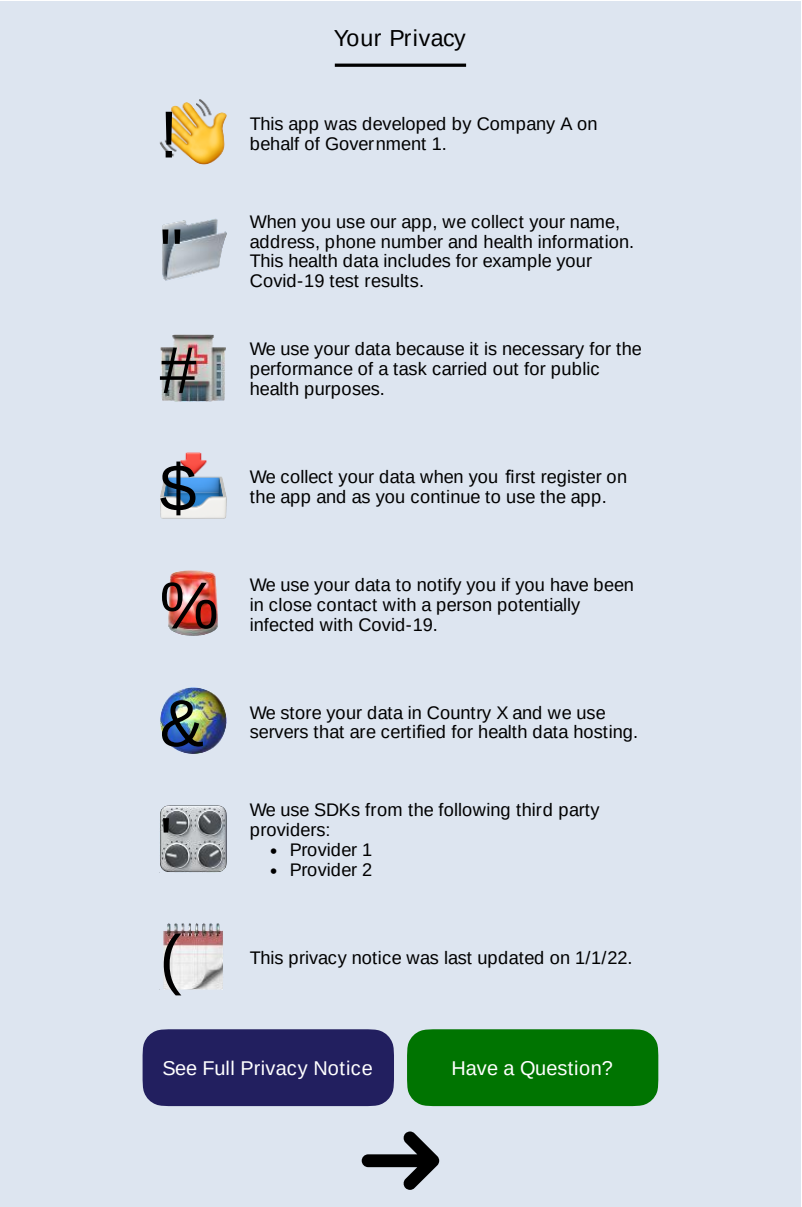
Шаблон карты потока персональных данных для приложения «Иммунный паспорт»

Карта потока персональных данных может использоваться для обеспечения связи правовых требований с конкретными этапами жизненного цикла данных, что позволит гарантировать соблюдение всех требований при их сборе и обработке. Ниже приведен пример карты, в которой указаны конкретные юридические требования, действующие на каждом этапе жизненного цикла данных, и функциональность, которой должно обладать приложение. Идентификатор требования должен соответствовать идентификатору, указанному в соответствующей спецификации требований к программному обеспечению для приложения, пример которой можно увидеть выше.

Жизненный цикл данных об информации о здоровье пользователя		
Этап жизненного цикла данных	**Идентификатор требования**	**Описание требования**
Сбор	REQ-51	Приложение обрабатывает статус вакцинации против Covid-19, результаты тестов на Covid-19 и информацию о естественном иммунитете от Covid-19. Такая медицинская информация собирается при регистрации и впоследствии, когда пользователь вводит информацию в приложение.
Использование	REQ-78	Приложение преобразует информацию о здоровье пользователя в QR-код, который пользователь может показать организаторам мероприятия, чтобы войти в заведение.
Раскрытие	REQ-09	Генерируется QR-код пользователя для сканирования операторами заведения.
Хранение	REQ-12	Медицинская информация пользователя сохраняется до тех пор, пока пользователь сохраняет приложение на своем устройстве. Приложение не сохраняет данные о месте, в котором был отсканирован QR-код пользователя.
Уничтожение	REQ-34	Информация о здоровье пользователя уничтожается при удалении приложения.

Шаблон уведомления о конфиденциальности для приложения по отслеживанию контактов

Ниже приведен пример краткой формы уведомления о конфиденциальности, которая может использоваться в приложениях по отслеживанию контактов и демонстрируется пользователям при первой регистрации в приложении. Цель состоит в том, чтобы предоставить наиболее важную информацию об обработке данных, осуществляемой приложением, с возможностью просмотреть полную версию уведомления или задать вопрос разработчику.



English Text	Translated Text
Your Privacy	Ваша конфиденциальность
This app was developed by [Company A] on behalf of [Government 1].	Приложение разработано [компанией A] для [правительства 1].
When you use our app, we collect your name, address, phone number and health information. This heath data includes for example your Covid-19 test results.	Когда вы пользуетесь нашим приложением, мы регистрируем ваше имя, адрес, номер телефона и медицинскую информацию. Эти медицинские данные включают, например, результаты теста на Covid-19.
We use your data because it is necessary for the performance of a task carried out for public health purposes.	Мы используем ваши данные, поскольку это необходимо для выполнения задачи, реализуемой в целях охраны здоровья населения.
We collect your data when you first register on the app and as you continue to use the app.	Мы собираем ваши данные, когда вы впервые регистрируетесь в приложении и при дальнейшем использовании приложения.
We use your data to notify you if you have been in close contact with a person potentially infected with Covid-19.	Мы используем ваши данные, чтобы уведомить вас, что вы находились в тесном контакте с потенциальным носителем Covid-19.
We store your data in [Country X] and we use servers that are certified for health data hosting.	Мы храним ваши данные в [стране X] и используем серверы, сертифицированные для размещения медицинских данных.
We use SDKs from the following third party providers: ● [Provider 1] ● [Provider 2]	Мы используем пакет SDK от следующих сторонних поставщиков: ● [Провайдер 1] ● [Провайдер 2]
This privacy notice was last updated on 1/1/22.	Дата последнего обновления настоящего уведомления о конфиденциальности - 01.01.22
See Full Privacy Notice	Полный текст уведомления о конфиденциальности
Have a Question?	Задать вопрос

Шаблон оценки воздействия на защиту данных/конфиденциальность

Ниже приведен шаблон оценки воздействия на защиту данных/ конфиденциальность, которую необходимо провести до внедрения приложения.

Система/Приложение	[…]
Система/Версия приложения	[…]
Дата проведения оценки воздействия на защиту данных	[…]

Общие сведения о проекте	
Что представляет собой разрабатываемая система/приложение?	[…]
С какой целью разрабатывается система/приложение?	[…]
Кто участвует в разработке системы/приложения?	[…]
Какие виды тестирования системы/ приложения были проведены?	[…]
Какова планируемая дата полного развертывания?	[…]

Описание операции обработки данных	
Какие персональные данные используются системой/приложением?	[…]
Для чего используются персональные данные?	[…]
Кому раскрываются персональные данные?	[…]
Какие SDK или другие библиотеки стороннего программного	

обеспечения используются для разработки системы/приложения?	

Выявление рисков			
Угроза	**Уязвимость**	**Событие**	**Риск**
[…]	[…]	[…]	[Низкий, средний или высокий]

Управление рисками			
Риск	**Реакция**	**Тип реакции**	**Обоснование**
[…]	[Принять, передать, ограничить или избежать]	[Технический, организационный или договорной]	[…]