гражданский СОЮЗ

ГРАЖДАНСКАЯ ИНИЦИАТИВА ИНТЕРНЕТ ПОЛИТИКИ

Аналитическая справка

«Безопасный город» - 2: защита персональных данных и перспективы развития проекта для профилактики правонарушений

Гражданский союз

Бишкек, 2022

Настоящая аналитическая справка подготовлена ОО «Гражданский союз» при поддержке ОФ «Гражданская инициатива интернет политики». Этот документ вытекает из результатов предыдущего исследования Гражданского союза («Проект «Безопасный город». Защита персональных данных и вопросы деперсонализации»), проведенного в 2021 году. Справка содержит анализ текущей ситуации вокруг ранее выработанных рекомендаций, а также обновленные рекомендации по дальнейшему совершенствованию работы АИС «Безопасный город» и защиты персональных данных при ее реализации.

Содержание

Список аббревиатур и сокращений

АИС - автоматизированная информационная система
АПК - аппаратно-программный комплекс
ГС - Гражданский союз
ГУВД - Главное управление внутренних дел
ГУОБДД - Главное управление обеспечения безопасности дорожного движения
ЕРП - Единый реестр преступлений
ЕРПн - Единый реестр правонарушений
ЕРПП - Единый реестр преступлений и проступков
ЖК - Жогорку Кенеш
КР - Кыргызская Республика
МВД - Министерство внутренних дел
МЦР - Министерство цифрового развития
НПА - нормативные правовые акты
ОО - общественное объединение
ОФ - общественный фонд
ПД - персональные данные
ПДД - правила дорожного движения
СМИ – средства массовой информации
УНП ООН - Управление Организации Объединенных Наций по наркотикам и преступности
УПСМ - Управление патрульной службы милиции

Введение

В 2021 году Гражданский союз провел исследование, посвященное вопросам безопасности персональных данных в автоматизированной информационной системе «Безопасный город» и перспективам использования открытых данных для профилактики правонарушений. Это исследование было направлено на изучение существующих пробелов в законодательстве и практике по защите персональных данных, существующих норм по обеспечению открытости данных, а также запуск публичных дискуссий вокруг этих вопросов.

В процессе обсуждения результатов исследования государственные органы начали реагировать на содержащиеся в документе рекомендации и замечания. Так, МВД заявило о приостановлении использования технологии распознавания лиц и отсутствии в будущем связи с системами, содержащими персональные данные всех граждан Кыргызстана[1]. И хотя формально данная система сейчас активно не используется, риск нарушения прав граждан при использовании этого и других технологических решений был и остается высоким.

Ряд рекомендаций предыдущего исследования уже нашли отражение в решениях государства, однако не все из них были реализованы должным образом. Учитывая планы государства по внедрению цифровых решений в сфере обеспечения общественной безопасности, вопросы законного и обоснованного использования персональных данных граждан должны находиться под пристальным вниманием гражданского общества. В связи с этим возникла необходимость актуализировать ранее представленные рекомендации с учетом реализации стратегических планов государства как на уровне законодательства и подзаконных актов, так и на уровне практического внедрения защитных мер. Важным остается развитие потенциала таких систем как «Безопасный город», ЕРП и ЕРПн в плане превенции правонарушений, поскольку имеющиеся массивы данных в обезличенном формате могут послужить основой для выработки более эффективных профилактических мер.

Государство, понимая значимость «Безопасного города» для обеспечения общественной безопасности, признает необходимость его дальнейшего развития. Так, в Национальной программе развития Кыргызской Республики до 2026 года[2] содержатся задачи, связанные с расширением географического охвата и функционала проекта с включением вопросов профилактики правонарушений и преступности в общественных местах. В рамках задачи по цифровизации управления и развития цифровой инфраструктуры планируется запуск фазы «Смарт города» как продолжение проекта «Безопасный город».

---

1 https://24.kg/obschestvo/216284_laquobezopasnyiy_gorodraquo_identifikatsiya_lits_vnbspkyirgyizstane_poka_nenbspprimenyaetsya/

2 утверждена Указом Президента Кыргызской Республики от 12 октября 2021 года № 435

Другой программный документ государства - Концепция государственной политики в сфере профилактики правонарушений на 2022-2028 годы[3] более подробно рассматривает расширение проекта «Безопасный город» как один из инструментов для решения задач профилактики правонарушений. Помимо этого в компонентах реализации Концепции содержится задача по развитию механизмов защиты персональных данных и открытости статистических обезличенных данных таких информационных систем как «Безопасный город», ЕРП, ЕРПн и других.

Наряду с планами по расширению функционала «Безопасного города» происходит процесс передачи этой автоматизированной системы в ведение Генеральной прокуратуры. Планируется внедрение других цифровых решений, связанных с обеспечением правопорядка, которые остро ставят вопрос соблюдения баланса между обеспечением безопасности и приватностью частной жизни граждан. Необходимо уделять пристальное внимание тому, как этот вопрос будет урегулирован. Появление профильного органа по защите персональных данных играет важную роль в этом процессе, однако проблемы сохраняются и не все из них могут быть решены на его уровне.

Подходы к защите персональных данных в будущем должны включать не только технические способы защиты от несанкционированного доступа и утечек, но и механизмы, позволяющие сохранять их конфиденциальность. Для этого необходимо обновление нормативных документов, внутриведомственных инструкций, постоянное обучение персонала, имеющего доступ к базам данных. При этом важно понимать, что исключительно за счет усиления технических методов защиты государство не сможет достичь доверия граждан по этому вопросу. Государство в целом и уполномоченный орган в частности, должны проводить и другую работу, направленную на повышение осведомленности граждан и понимание важности приватности личных данных в век цифровых технологий.

Прогрессивным шагом является намерение государства развивать инициативу открытых данных и их использование для более эффективного государственного управления. Однако часть значимой информации относительно ситуации с общественной безопасностью может оставаться недоступной. Основная причина связана с излишней засекреченностью работы правоохранительных органов и их закрытостью в целом. В этой связи, продолжают оставаться актуальными рекомендации по обеспечению открытости и прозрачности их деятельности, в том числе по вопросам публикации открытых данных и сотрудничества с гражданским обществом для совместной аналитической работы и выработке решений.

[3] утверждена постановлением Кабинета Министров Кыргызской Республики от 23 августа 2022 года № 469

По защите персональных данных в АИС «Безопасный город»

Текущие процессы и изменения

Текущие процессы вокруг «Безопасного города» показывают, что его рассмотрение с точки зрения защищенности персональных данных выходит за рамки самого проекта и затрагивает более широкий круг вопросов, чем в предыдущем исследовании. На момент подготовки данного документа, происходила передача АИС «Безопасный город» Министерством цифрового развития в ведение Генеральной прокуратуры Кыргызской Республики. Это связано с принятием в 2021 году нового уголовного законодательства и введением в действие новых версий автоматизированных информационных систем «Единый реестр преступлений» и «Единый реестр правонарушений», держателем и координирующим органом которых является Генеральная прокуратура[4].

По информации представителей МЦР, процесс передачи затянулся. Согласно Постановлению Кабинета министров от 6 июня 2022 года[5], этот процесс должен был происходить при содействии межведомственной комиссии, образовать которую было поручено Министерству цифрового развития. Планируется, что все совершенные правонарушения, включая зафиксированные с применением АПК в рамках реализации «Безопасного города» будут фиксироваться в «Едином реестре правонарушений» за счет объединения этих двух систем. Таким образом предполагается формировать единую статистическую базу.

Положение о Едином реестре правонарушений согласно законодательству должно определяться Генеральным прокурором КР и утверждаться Кабинетом министров, однако на момент подготовки справки этот документ отсутствовал в открытом доступе. Это может быть связано с затянувшимся процессом инвентаризации и приведения законодательства в соответствие с новой редакцией Конституции и новым уголовным законодательством. Если данное положение еще не принято, важно, чтобы в нем по аналогии с пока действующим Положением о ведении Единого реестра нарушений были отражены нормы, связанные с защитой персональных данных, находящихся в данной системе или смежных с ней.

[4] Конституционный Закон Кыргызской Республики от 10 сентября 2021 года № 114 «О прокуратуре Кыргызской Республики»

[5] Постановление Кабинета министров Кыргызской Республики «Об утверждении Порядка формирования и использования сумм штрафов, взысканных за совершение правонарушений, обработанных в автоматизированной информационной системе «Единый реестр правонарушений», в том числе зафиксированных с применением аппаратно-программного комплекса, в рамках реализации компонента «Безопасный город» проекта «Умный город»

В исследовании 2021 года[6] поднимался вопрос отсутствия единого концептуального видения как развития проекта «Безопасный город», так и вопросов перспектив развития цифровых технологий для обеспечения дорожной и общественной безопасности в целом. И хотя на данный момент развитию «Безопасного города» как самостоятельного проекта в программных документах государства уделяется мало внимания, его функционал планируется расширить для более эффективного решения задач по профилактике правонарушений и преступности в общественных местах.

Последние решения относительно «Безопасного города» и внедрение новых технологических решений являются важными с точки зрения обеспечения общественной безопасности, однако оставляют вопросы, на которые общество пока не может получить ответы из-за их разрозненного применения. Отсутствие единой, понятной обществу стратегии цифровизации в области обеспечения общественной безопасности также сохраняет существующие правовые пробелы в области защиты персональных данных, способствующие нарушению прав граждан.

В 2022 году для обеспечения безопасности дорожного движения появились нововведения, которые в свете объединения нескольких информационных систем можно рассматривать как составную часть «Безопасного города». Так, запущена система комплексов фото- и видеофиксации нарушений ПДД «АвтоУраган», им оснащены патрульные машины[7].

Система используется для фиксации нарушений и розыскных мероприятий, а также активно применяется для контроля авто трафика на трассах и перекрестках. Она может считывать номера автомобилей, идентифицировать их, архивировать и хранить информацию, проверять распознанные номера по подключенным базам данных и передавать сведения оператору[8]. Таким образом, находящиеся в патрульной машине сотрудники могут получать из подключенных баз данных информацию о транспортных средствах в поле видимости камеры и сохранять новые нарушения.

Для фиксации нарушений и взыскания неоплаченных штрафов в рамках «Безопасного города» с июля 2022 года сотрудники УПСМ по ГУВД г. Бишкек также начали использовать планшеты. Это нововведение ускоряет процесс проверки документов правонарушителей в режиме онлайн и позволяет вести производство

[6] Здесь и далее: выделенный текст содержит общее описание рекомендаций предыдущего исследования и выводы относительно текущей ситуации, связанной с выполнением/невыполнением данных рекомендаций

[7] https://24.kg/obschestvo/237542_novuyu_sistemu_poiska_narushiteley_zapustili_nadorogah_kyirgyizstana/

[8] https://24.kg/obschestvo/232235_sistema_avtouragan_ustanovlena_napatrulnyih_mashinah_dlya_fiksatsii_narushenij/

дел в электронном формате. Планшеты подключены к базам данных, содержащим персональные данные граждан.

По информации пресс-службы МВД, до сентября 2022 года было задействовано 23 планшета. 14 сентября 2022 года УНП ООН вручил МВД 195 планшетов[9], которые будут переданы во все подразделения ГУОБДД. Позднее на заседании Комитета ЖК по правопорядку, борьбе с преступностью и противодействию коррупции начальник ГУОБДД МВД Азамат Исраилов сообщил, что до конца года ведомство планирует получить 500 планшетов через спонсорскую помощь[10].

Поскольку использование системы «АвтоУраган» и планшетов сотрудниками подразделений ГУОБДД предполагает доступ к базам, в том числе содержащим персональные данные граждан, использование этих технологий должно регулироваться в соответствии с нормами Закона КР «Об информации персонального характера», чтобы исключить случаи утечки или неправомерного использования этих данных.

В исследовании Гражданского союза 2021 года рассматривались особенности защиты персональных данных при использовании АПК, фиксирующих нарушения ПДД. Эти данные отправлялись в Центр обработки данных, где автоматизированная система обрабатывала полученные файлы и сопоставляла их с базами по национальным паспортам, адресам официальной прописки, базой транспортных средств. Обработкой и оформлением протоколов занимались уполномоченные сотрудники Центра мониторинга ГУОБДД.

Таким образом, в случае со стационарными АПК обработка персональных данных проводилась в закрытой сети, в отдельном специализированном помещении и доступ к персональным данным имели только уполномоченные сотрудники. Но и в этом случае фиксировались факты утечек, в связи с чем в рекомендациях поднимался вопрос усиления основных правовых, организационных и технических мер защиты персональных данных. Эти же меры должны быть применимы к использованию таких систем как «АвтоУраган», а также при использовании сотрудниками планшетов, связанных с базами персональных данных.

Предполагается, что с передачей АИС «Безопасный город» в ведение Генеральной прокуратуры технический порядок обработки данных также будет исключать возможность несанкционированного доступа к данным. Однако, пока не ясно, каким образом эти системы будут интегрированы, каким образом будет обрабатываться информация с АПК, позволяющая отслеживать перемещение

[9] https://24.kg/obschestvo/245080
[10] https://kg.akipress.org/news:1808773

транспорта и в ведении какого органа будут находиться действующие центры обработки данных.

Как и ранее, главной уязвимостью является человеческий фактор. Сотрудники могут использовать доступ в незаконных целях в результате подкупа или по собственной инициативе, не исключается также влияние на них с целью политического преследования отдельных лиц.

Постановлением Правительства Кыргызской Республики от 22 декабря 2021 года №325 было утверждено Положение о Государственном агентстве по защите персональных данных при Кабинете Министров Кыргызской Республики, 10 января 2022 года агентство зарегистрировано в органах юстиции.

Государственное агентство по защите персональных данных является государственным органом исполнительной власти, разрабатывающим и реализующим единую государственную политику в сфере информации персонального характера. Оно должно также выполнять функции по обеспечению защиты прав субъектов персональных данных, регистрации держателей массивов персональных данных и ведению Реестра держателей. На момент подготовки данного документа, в Реестре значилось 159 держателей массивов персональных данных, из них 146 - государственные организации, 13 - коммерческие структуры[11]. При этом большая часть записей была недоступна для просмотра, что может быть связано с необходимыми процедурами оформления в реестре и согласования с держателем.

Министерство внутренних дел, как и другие правоохранительные органы в Реестре отсутствуют. Это связано с тем, что в отношении имеющихся в правоохранительных органах и органах прокуратуры массивов данных правовой режим устанавливается в соответствии с законами Кыргызской Республики «Об оперативно-розыскной деятельности» и «О защите государственных секретов Кыргызской Республики».

В исследовании 2021 года было рекомендовано обеспечить независимость уполномоченного органа и ориентировать его работу прежде всего на мониторинг, информационную работу, а также создание и поддержание условий для большей защищенности данных. Большие ожидания были связаны также с тем, что данный орган будет иметь возможность надзора за правоохранительными органами в части правомерности использования персональных данных.

По факту функции Государственного агентства в сфере регулирования, координации, надзора и контроля не распространяются на персональные данные,

[11] https://dpa.gov.kg/ru/register

полученные в результате деятельности органов прокуратуры Кыргызской Республики, правоохранительных органов и органов, осуществляющих оперативно-розыскную, разведывательную и контрразведывательную деятельность, производство официальной статистики.

Надзорные функции уполномоченного органа оказались урезанными именно в той части, где они являются наиболее существенными и необходимыми для защиты персональных данных граждан не только от несанкционированного доступа, но и с точки зрения возможности использования данных в противоправных целях самими правоохранительными органами. Данные опасения усиливаются на фоне возрастающего давления на свободу слова, а также массового задержания политиков и активистов в октябре 2022 года.

Однако Министерство внутренних дел и отдельные государственные учреждения при нем являются держателями массивов, которые ранее, находясь в ведении «гражданских» структур, не относились к государственным секретам. Так, например, в конце 2021 года было принято решение передать Государственное учреждение «Унаа» при Министерстве цифрового развития в ведение Министерства внутренних дел с соответствующим штатом, материально-технической базой и финансовыми средствами. Были также переданы отдельные функции других министерств и ведомств.

Поскольку целью учреждения «Унаа» является реализация государственной политики в области регистрации, и перерегистрации транспортных средств, выдачи водительских удостоверений, допуска водителей к управлению транспортными средствами, соответствующая база с персональными данными теперь находится в распоряжении у подведомственного МВД учреждения. Это обязывает его пройти соответствующую регистрацию в Реестре держателей, поскольку эти данные не относятся к данным, полученным в ходе оперативно-розыскной, разведывательной и контрразведывательной деятельности. С указанной базой данной непосредственно связана работа проекта «Безопасный город», системы «АвтоУраган» и другие технические решения, направленные на обеспечение дорожной безопасности.

В случае с Министерством внутренних дел, по-прежнему остается нерешенным вопрос дальнейшего использования и получения данных при работе с системой распознавания лиц. В ответ на официальный запрос в ведомстве пояснили, что согласно распоряжению МВД КР работа Центра оперативного управления Службы общественной безопасности по линии идентификации лиц по камерам видеонаблюдения с функцией распознавания лиц приостановлена с 18 октября 2021 года. Министерство цифрового развития, в свою очередь сообщило, что данная функция была заложена на долгосрочную перспективу. На круглом столе, посвященном обсуждению данной аналитической справки, представителями МВД было озвучено, что пилотный проект по розыску совершивших преступления и пропавших без вести запущен заново на базе Центра оперативного управления.

Используется российское программное обеспечение с функцией распознавания лиц в тестовом режиме, в случае успешного тестирования данная программа будет приобретена для постоянного использования.

В исследовании 2021 года было озвучено, что использование технологии распознавания лиц как в рамках «Безопасного города», так и вне его не урегулировано в НПА. Отсутствует информация о целях сбора таких данных, их связи с другими персональными данными, способах обработки и хранения. Данная технология не может использоваться до тех пор, пока не будут разработаны и приняты соответствующие документы и решения.

На данный момент в открытом доступе отсутствует информация о работе в данном направлении как уполномоченного органа по защите персональных данных, так и других государственных органов. Учитывая, что ранее внедрение технологии происходило не только без соответствующей правовой базы, но и без общественных обсуждений инициативы, существует риск, что этот вопрос будет оставаться полностью закрытым для общественности, что будет усугублять опасения относительно неправомерного использования технологии правоохранительными органами.

Запланированы изменения, связанные с закреплением ответственности должностных лиц, имеющих доступ к персональным данным, в том числе в рамках «Безопасного города» и других информационных систем. В этом направлении Государственным агентством по защите персональных данных был разработан проект Закона «О внесении изменений в некоторые законодательные акты по вопросам защиты персональных данных»[12].

В сопроводительных документах к данному законопроекту[13] обозначено, в условиях цифровой трансформации органы государственной власти не могут обеспечить режим законности из-за отсутствия юридических оснований для привлечения к ответственности лиц, виновных в нарушении законов. Для устранения этого пробела планируется внесение в Кодекс о правонарушениях изменений, вытекающих из требований Закона Кыргызской Республики «Об информации персонального характера».

В частности, предусматривается введение новой статьи 413-1 (Нарушение требований о защите персональных данных), устанавливающей ответственность за нарушение установленного законодательством порядка сбора, хранения, обработки, использования, защиты, передачи, распределения или распространения информации персонального характера. Также этой статьей предлагается закрепить ответственность за необоснованный отказ в

[12] https://dpa.gov.kg/ru/npa/20
[13] https://dpa.gov.kg/ru/npa/20, http://koomtalkuu.gov.kg/ru/view-npa/1999

предоставлении субъекту персональных данных информации, касающейся обработки его персональных данных.

Также закрепляется ответственность за нарушение установленного законом порядка трансграничной передачи персональных данных. Отдельным пунктом прописано внесение неполной или недостоверной информации в Реестр держателей массивов персональных данных, а равно сбор, хранение, обработка персональных данных без соответствующей регистрации в Реестре. Одной из переходных норм является закрепление ответственности за нарушения при сборе, хранении и обработке персональных данных без использования средств автоматизации, поскольку в ближайшие десятилетия практика сбора, хранения и обработки персональных данных может быть полностью заменена на автоматизированную обработку[14].

Законопроектом также предложено определить Государственное агентство по защите персональных данных как орган, который будет выявлять нарушения законодательства, рассматривать дела и налагать взыскания по правонарушениям, предусмотренным статьями 228 (Неправомерный доступ к компьютерной информации), 228-1 (Нарушение требований по защите информации персонального и коммерческого характера) и 413-1 (Нарушение требований о защите персональных данных).

В справке-обосновании к проекту закона указано, что этот шаг обоснован необходимостью разграничить полномочия и передать административную часть работы по возбуждению дел о правонарушениях и рассмотрению их в ведение уполномоченного государственного органа по персональным данным, поскольку статьи 228 и 228-1 напрямую не направлены на общественный порядок и данные нормы используются органами внутренних дел в незначительной степени.

В исследовании 2021 года поднималась не только необходимость урегулирования вопросов ответственности должностных лиц, имеющих доступ к персональным данным, в том числе в рамках «Безопасного города», но и вопросы определения ущерба, который может быть причинен человеку в результате разглашения его персональных данных, и, соответственно, компенсации этого ущерба, что пока не было сделано.

Также была обозначена необходимость ускорения принятия документов, которые помогут сделать систему защиты персональных данных надежнее, а политику их обработки - прозрачнее. Речь шла о перечне угроз безопасности, методике определения угроз и формы, согласно которым каждый владелец массивов персональных данных должен оценивать угрозы безопасности и устранять их. В рамках предыдущего исследования респонденты неоднократно ссылались на

[14] https://dpa.gov.kg/ru/npa/20

скорый запуск работы отдельного уполномоченного органа, который должен решить эти вопросы.

На данный момент документы пока не приняты, что будет осложнять отдельные аспекты защиты персональных данных уполномоченным органом. Кроме того, остается нерешенным вопрос выявления нарушений со стороны правоохранительных органов, поскольку у Государственного агентства по защите персональных данных недостаточно полномочий для надзора и контроля за ними.

Государственное агентство инициировало принятие Положения об Учебном центре, который будет реализовывать программы дополнительного образования в области информации персонального характера, информационной безопасности, цифрового права, кибер гигиены и цифровых навыков. Кроме того, деятельность центра должна будет способствовать обеспечению держателей массивов персональных данных квалифицированными сотрудниками, ответственными за сохранность массивов персональных данных, правовое, организационное и техническое обеспечение сбора, хранения и обработки персональных данных. Постановление Кабинета Министров Кыргызской Республики №540 «Об Учебном центре Государственного агентства по защите персональных данных при Кабинете Министров Кыргызской Республики» было утверждено 27 сентября и вступило в силу 18 октября 2022 года[15].

В исследовании 2021 года было отмечено, что важным шагом к большей защищенности персональных данных должна стать система обучения, переподготовки и повышения квалификации сотрудников для работы с персональными данными, привлечения лучших специалистов для определения угроз и выстраивания системы защиты. Это направление отмечалось как приоритетное не только с точки зрения защищенности персональных данных, но и с позиции внедрения цифровых технологий в целом, поскольку имеет значительное влияние на качество работы информационных систем, таких как «Безопасный город», ЕРП, ЕРПн и других.

Несмотря на предпринятые шаги в данном направлении, сфера влияния Государственного агентства ограничена, в связи с чем остается неясным, будет ли деятельность Учебного центра охватывать правоохранительные органы, в том числе непосредственного владельца АИС «Безопасный город».

[15] https://dpa.gov.kg/ru/npa/12

Рекомендации

- Необходимо принятие единой концепции применения цифровых решений как в рамках профилактики преступности, так и в целом в области управления государством. Она должна включать стратегию развития информационных систем с четко определенными целями, задачами и индикаторами достижения результатов, которая поможет гражданскому обществу отслеживать, насколько государство отходит от первоначальных целей использования этих систем, насколько внедрение новых технологий соответствует и соразмерно этим целям и не нарушает ли права граждан, а также отслеживать любые изменения в задачах и целях, с которыми персональные данные собираются и обрабатываются, используются и хранятся. Широкие консультации при подготовке данного документа и размещение его в открытом доступе снимет большинство вопросов, которыми задается общество и позволит повысить доверие к государству в вопросах применения цифровых технологий.

- Актуальным остается усиление в нормативных и ведомственных актах норм, связанных с защитой персональных данных. С 2017 года действуют Требования к обеспечению безопасности и защите персональных данных при их обработке в информационных системах персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных. В виду передачи АИС «Безопасный город», рекомендации касаются в большей степени таких систем как ЕРП, ЕРПн и смежных с ними. Эти нормы должны быть отражены также в инструкциях подразделений правоохранительных органов, которые имеют доступ к базам с персональными данными граждан. При этом особое внимание необходимо уделять таким вопросам как:
    - контроль за доступом (исключение доступа посторонних лиц к оборудованию, которое используется для обработки ПД);
    - контроль за пользованием (препятствие самовольному чтению, копированию, изменению или выносу носителей данных);
    - контроль за средствами передачи данных (обеспечение безопасности систем обработки данных, которые подлежат передаче, независимо от средств передачи данных);
    - контроль за допуском (обеспечение доступа каждого пользователя системы к ПД только в пределах его уровня допуска);
    - транспортный контроль (исключение возможностей несанкционированного чтения, копирования, изменения или уничтожения ПД при передаче и транспортировке данных).

- Необходимо законодательно закрепить за Государственным агентством по защите персональных данных функции надзора за правоохранительными органами в области защиты персональных данных.

- С учетом рисков, которые связаны с защитой персональных данных при применении цифровых решений в сфере обеспечения безопасности, необходимо расширить сферу влияния Государственного агентства по защите персональных данных, чтобы охватить вопросы обработки и использования ПД правоохранительными органами. Для этого рекомендуется рассмотреть вариант придания органу независимого статуса как парламентского института, в этом случае орган будет выполнять функции «информационного омбудсмена» с постоянной отчетностью перед парламентом.

- Поскольку правовой статус использования технологии распознавания лиц до сих пор не установлен, а также с учетом планов по расширению функционала «Безопасного города» уполномоченному органу по защите персональных данных необходимо разработать систему критериев и условий, при соблюдении которых данная система может функционировать без ущерба правам граждан и без рисков для персональных данных. При этом сервер рекомендуется размещать в управлении «гражданского» министерства (например, Министерства цифрового развития), а не в правоохранительных органах, чтобы снизить риски неправомерного использования технологии.

По перспективе обезличивания данных для профилактики правонарушений

Текущие процессы и изменения

Практика применения данных из информационных систем, в том числе АИС «Безопасный город», при принятии решений в секторе правопорядка пока не получила распространения. Однако по процессам, связанным с развитием политики открытых данных в целом, в Кыргызстане наметились положительные тенденции. В то же время вопросы относительно открытости данных о состоянии общественной безопасности по-прежнему остаются.

В исследовании 2021 года было отмечено, что в концептуальных документах государства нет понятного курса на на обеспечение открытости статистических данных правоохранительной направленности.

В качестве решения Гражданским союзом предлагалось принятие стратегии по открытым данным и включение положений об открытых данных в программах по реформам в правоохранительных органах.

В сентябре 2022 года была принята Концепция открытых данных[16]. В целях концепции указано, что она «в полной мере соответствует Национальной стратегии развития Кыргызской Республики до 2026 года», где в качестве приоритета содержится совершенствование законодательных основ и организационных механизмов участия гражданского общества в процессах принятия решений, а раскрытие государственными органами информации в форме открытых данных является одной из базовых задач при совершенствовании государственного управления и формировании «Открытого Правительства».

Концепция содержит основные принципы открытых данных, среди которых значатся:

- открытость - государственные органы раскрывают данные по умолчанию и по своему выбору; доступ обеспечивается ко всем данным, за исключением особых категорий данных (доступ к которым ограничен в соответствии с законом);
- защита безопасности охраняемой законом информации - государственные органы должны придерживаться принятой государственной политики (в

[16] утверждена Распоряжением Кабинета Министров Кыргызской Республики от 2 сентября 2022 года № 463-р

области цифрового развития, электронного управления, информатизации, защиты информации и данных, доступ к которым ограничен в соответствии с законодательством КР);

- доступность - государственные органы должны обеспечить для всех граждан такой формат раскрытия данных, который позволит свободно производить поиск, копировать и распространять открытые данные по своему усмотрению, без каких-либо ограничений для последующего использования; данные должны быть доступны в сети Интернет широкому кругу пользователей без требования о регистрации;

- ответственность государственных органов, являющихся обладателями информации - государственные органы должны отвечать за качество публикуемых данных, в том числе за достоверность, полноту и своевременное обновление (с установленной периодичностью);

- повторное использование - данные будут предоставляться пользователю на портале открытых данных в форматах, дающих возможность автоматически обрабатывать и скачивать для повторного использования в целях, которые не противоречат законодательству КР;

- приоритетность и очередность при опубликовании - в связи с ограниченностью ресурсов размещать информацию на портале открытых данных будут с учетом ее востребованности обществом.

В рамках последнего из вышеперечисленных принципов предполагается, что государственные органы будут взаимодействовать с гражданским обществом, средствами массовой информации, исследователями, разработчиками и другими заинтересованными сторонами, чтобы установить, какие данные являются приоритетными.

В исследовании 2021 года отмечалось, что обеспечение открытости данных о ситуации с общественной безопасностью, дорожной безопасностью и преступностью должно стать одним из приоритетных направлений профилактики правонарушений, при этом «Безопасный город» должен стать одним из источников информации, но не единственным.

АИС «Безопасный город» уже на том этапе была призвана аккумулировать данные, которые должны использоваться для анализа и прогнозирования. Текущие планы по увеличению охвата и функций системы, а также ее интеграция с ЕРПн расширяют возможности для такого рода работы.

Закон Кыргызской Республики «Об основах профилактики правонарушений» содержит норму, согласно которой общая профилактика (то есть профилактика, которая направлена на все общество) осуществляется путем проведения

исследований и анализа криминологической статистики[17]. 23 августа 2022 года во исполнение данного закона была принята Концепция государственной политики в сфере профилактики правонарушений на 2022-2028 годы. Отдельное направление Концепции посвящено внедрению цифровых технологий в профилактическую деятельность.

Одна из задач данного направления включает использование технологических решений, которые позволят субъектам профилактики анализировать данные о преступлениях и правонарушениях, складывающейся ситуации в общественных местах и на дорогах, а также о криминогенных тенденциях. Она включает картирование инцидентов и их анализ, развитие аналитического модуля в системах ЕРП, ЕРПн, «Безопасного города», создание «тепловых карт» для обозначения криминогенных и проблемных районов. Таким образом предполагается создание условий для принятия субъектами профилактики более эффективных решений, основанных на данных.

Ведущим актором в процессе предоставления открытых данных о ситуации с общественной безопасностью является Генеральная прокуратура КР, как орган, отвечающий за формирование государственной правовой статистики. Кроме того, ГП ведет и является держателем ЕРП и ЕРПн. Помимо этого, согласно законодательству, ГП устанавливает единый порядок формирования и представления отчетности правоохранительными и иными государственными органами, а также анализирует и прогнозирует состояние преступности с выработкой тактики и методики борьбы с ней.

Конституционный закон «О прокуратуре Кыргызской Республики» определяет также осуществление информационно-аналитической деятельности ГП (с использованием системы информационного обмена правоохранительных и иных государственных органов). Эта деятельность проводится в целях выявления негативных явлений для выработки мер, в том числе законодательных, направленных на профилактику правонарушений; установления количественных и качественных сведений о фактах нарушений законности в различных сферах правоотношений, выработки предложений по профилактике и пресечению этих явлений; изучения и переработки сведений, характеризующих состояние законности и правопорядка, в том числе в разрезе регионов. При этом в законе уже заложена норма об использовании сведений для информационно-аналитической работы в обезличенном виде, без раскрытия конкретных персональных данных физических лиц. Проведение аналитической деятельности с использованием персональных данных физических лиц требует наличия приказа Генерального прокурора, который принимается для каждого случая отдельно[18].

Информационно-аналитическая деятельность осуществляется органами прокуратуры в рамках надзорной функции в соответствии с планами аналитической

[17] подпункт 3 статьи 16 Закона КР "Об основах профилактики правонарушений"
[18] часть 4 статьи 47 Конституционного закона "О прокуратуре"

работы, утверждаемыми Генеральным прокурором. Закон также предусматривает внеплановое проведение такой работы, основаниями для которой могут быть поручения Генерального прокурора или его заместителей; мотивированные запросы Президента, комитетов ЖК, комиссий, образованных ЖК с целью проведения парламентского расследования. С согласия Генерального прокурора и его заместителей такая аналитическая работа может быть проведена по обоснованным запросам государственных органов, а по запросу депутата Жогорку Кенеша - только с согласия Генерального прокурора.

В исследовании 2021 года отмечалось отсутствие четкого определения о необходимости обеспечения открытости данных правоохранительной направленности. Это приводит к тому, что держатели статистики не только не ставят перед собой соответствующих задач по анализу и обеспечению открытости, но и неохотно дают статистику другим государственным структурам, парламентским комитетам и гражданскому обществу, например через затягивание или предоставление неполной информации.

Хотя обновленная версия профильного закона, принятого в 2021 году, расширила возможности для проведения Генеральной прокуратурой аналитической деятельности по запросам государственных органов, депутатов и комитетов ЖК, этого может оказаться недостаточно для необходимого уровня взаимодействия правоохранительных и других структур в целях анализа уголовно-правовой статистики и принятия обоснованных решений по профилактике. В этой связи передача всех систем, собирающих статистические данные о ситуации с общественной и дорожной безопасностью в ведение Генеральной прокуратуры усиливает риск того, что данные не будут доступны общественности.

Являясь владельцем АИС «Безопасный город» Министерство цифрового развития опубликовало на портале открытых данных деперсонализированные реестры нарушений ПДД, зафиксированные за период с марта 2019 по апрель 2021 года. Данные включают информацию о виде нарушения, сумме выписанного штрафа, марке автомобиля и участке автодороги, на котором нарушение зафиксировано. С момента открытия портала открытых данных ГП не была на нем зарегистрирована. Готовность Генеральной прокуратуры публиковать аналогичным образом открытые данные «Безопасного города», ЕРПн и ЕРП ставятся под сомнение из-за общей закрытости данного органа от общества.

Фактически, реестр нарушений ПДД стал единственным опубликованным массивом данных в сфере правопорядка на данном портале. Пакеты данных, размещенные Национальным статистическим комитетом, не содержат информации о состоянии преступности, хотя официальный сайт НСК позволяет найти данную информацию. Однако массивы НСК имеют ограниченный характер по видам преступлений, не включают в себя правонарушения и не позволяют увидеть дезагрегированную статистику по регионам.

Официальный сайт Генеральной прокуратуры содержал раздел со статистикой, однако, как и в случае с НСК, круг вопросов и период был ограничен. Кроме того, данные размещались в виде картинок, а не в машиночитаемом формате, что не соответствует требованиям, предъявляемым к открытым данным. Длительное время наблюдаются сложности с доступом к официальному сайту Генеральной прокуратуры, что не позволяет оценить текущее положение дел.

В 2021 году, в период действия старой системы ЕРПП, в ГП сообщали, что она позволяет сотрудникам правоохранительных органов получать мгновенно и в режиме онлайн сведения о зарегистрированных преступлениях и проступках по всей республике, производить фильтрацию записей по заданным параметрам. Планировалось также, что при последующей оптимизации функционал системы позволит обрабатывать объемные массивы данных за короткое время, на основе чего можно будет проводить глубокий анализ состояния преступности и принимать действенные меры по предупреждению и пресечению правонарушений[19].

О практической реализации данного компонента до разделения системы на ЕРП и ЕРПн, равно как о предложенных Генеральной прокуратурой мер по предупреждению преступности, нет информации в открытом доступе. Неясным остается также каким образом эти задачи будут реализованы в текущих условиях.

19 https://www.vb.kg/doc/395824_genprokyratyra_kr_ob_operativnosti_i_prozrachnosti_raboty_pravoohraniteley.html

Рекомендации

- В стратегических планах государства по цифровизации госуправления, обеспечению открытых данных и реформам в правоохранительных органах необходимо более четко обозначить курс на обеспечение открытости деперсонализированных данных правоохранительной направленности. Уточняющие нормы должны быть также внесены в законодательные и ведомственные акты, чтобы обозначить технические, инфраструктурные и иные задачи, связанные с работой в данном направлении.

- Поскольку у должностных лиц нет ясного понимания в чем заключается польза от обеспечении открытости данных, необходимо обеспечить в рамках реализации Концепции открытых данных и Концепции государственной политики в сфере профилактики правонарушений информационную работу и обучение личного состава правоохранительных органов, штабных работников, сотрудников ОМСУ по планированию на основе анализа данных. Частью этого процесса должно стать закрепление в этих органах сотрудников, ответственных за регулярную публикацию и обновление открытых данных, а также за налаживание сотрудничества с экспертными и научными кругами, гражданским обществом в целях поиска оптимальных решений.

- Гражданскому обществу, СМИ, исследователям, экспертным и научным кругам, а также иным заинтересованным лицам необходимо сформировать четкий запрос к государству по открытости данных о ситуации с общественной безопасностью и правопорядком. Это поможет актуализировать вопрос перед Генеральной прокуратурой и получить соответствующие ожиданиям данные в формате и объеме, подходящем для всестороннего анализа.

- Важным шагом при реализации Концепции открытых данных и Концепции государственной политики в сфере профилактики правонарушений должно стать обучение представителей гражданского общества, СМИ и других заинтересованных сторон анализу массивов данных о ситуации с общественной безопасностью и правопорядком с участием представителей государственных органов - держателей информации.