

04 июля 2019

Три года ждут: что угрожает обещанным цифровым паспортам россиян

Правительство утвердило проект электронного паспорта гражданина РФ, приоритетной названа концепция НИИ «Восход» и «Гознака». Это значит, что паспорт, вероятно, заменят на пластиковую карту с чипом и мобильное приложение. Выдавать первые электропаспорта должны, по планам Минкомсвязи, уже через год, однако аналитики и участники рынка сомневаются в полноценном запуске проекта и предупреждают об угрозах утечки персональных данных.

Вице-премьер РФ Максим Акимов поддержал концепцию электронного паспорта, предложенную Минкомсвязью, пишет 4 июля РИА Новости со ссылкой на источник, знакомый с ситуацией. В свою очередь, источники ТАСС сообщили, что речь идет о проекте, разработанном НИИ «Восход» и «Гознаком». Таким образом, на данном этапе согласований заменой российскому бумажному паспорту стала пластиковая карта с чипом, на котором будут содержаться данные действующих паспортов, отпечаток пальца, электронная подпись, а также защищенное мобильное приложение с доступом к госуслугам.



Кто именно займется созданием инфраструктуры этой системы, а также обеспечением ее безопасности, пока не сообщается, но уже через год должна быть выпущена первая партия, а через 9 лет бумажных паспортов не будет вовсе. На фоне масштабных утечек данных россиян и заявлений ЦБ об уязвимости к кибератакам даже крупнейших банков РФ аналитики ставят под вопрос поставленные кабмином сроки и запуск системы цифровых паспортов в целом.

В поисках формфактора

Вице-премьер Акимов одобрил концепцию электронного паспорта на профильном совещании 3 июля. На нем были названы и примерные сроки реформы: электронные удостоверения личности (ЭУЛ) начнут выдавать через год, в июле 2020 года, выпуск бумажных паспортов прекратится в начале 2023 года, а замена их на цифровые запланирована к концу 2028 года. При этом, согласно планам программы «Цифровая экономика», выдача электронных паспортов должна начаться в 2021 году, а бумажные удостоверения личности перестанут выдавать с 2025 года. То есть в правительстве намерены ускорить этот процесс. К слову, с 2021 года оцифровать все трудовые книжки 4 июля распорядился премьер Дмитрий Медведев.

Как утверждают осведомленные источники «Ведомостей», концепция ЭУЛ представляет собой две версии паспорта – на пластиковой карте с чипом и в защищенном мобильном приложении. Доступ в приложение пользователь получит одновременно с картой. Концепцию разработали НИИ «Восход» (подведомственен Минкомсвязи) и «Гознак».



Карта с чипом предусматривает хранение паспортных данных, отпечатка пальца и электронной подписи. В приложении будет содержаться копия паспорта, а также доступ к цифровому профилю гражданина и его электронной подписи. Цифровой профиль, в свою очередь, должен заработать к концу 2023 года (то есть тогда, когда перестанут выдавать обычные паспорта). Он объединит все данные госорганов, что позволит, в частности, автоматически заполнять любые формы при доступе к госуслугам, получать налоговые вычеты или предъявлять ГИБДД виртуальные права.

Источники РБК уточняют, что выдавать ЭУЛ строго вместо паспорта начнут с 2025 года. Этот же срок упоминался в распоряжении правительства России от 19 сентября 2013 года, утвердившем первую концепцию перехода на электронное удостоверение личности. В нем отмечалось, что с 2030 года бумажные паспорта перестанут действовать. Однако, по словам источника, в правительстве допускают, что ранее выданные паспорта будут использоваться до истечения их срока.

«Дольше ждать мы не можем, иначе у нас встанет вся инфраструктура. Мы не понимаем, с каким формфактором имеем дело, если не решим, каким будет дизайн электронного паспорта», – говорил в начале июня Акимов. По словам источника РБК, рассматривалось три варианта: пластиковая карта с чипом и мобильное приложение, только карта или только приложение.

Первые два варианта предлагает «Гознак» и «Восход», и, как следует из данных источников ТАСС и РИА Новости, эти варианты стали приоритетными. «Ростелеком» предлагал создать только защищенное мобильное приложение и сэкономить на выпуске карт, что оставляло нерешенным вопрос с доступом

к документу без электричества. Каждая из компаний претендует на статус оператора системы — структуры, которая организует взаимодействие между ведомствами, задействованными при выдаче паспорта.

«Гознак» предлагает окупать свои карты с чипом за счет граждан (например, сборами за подтверждение личности при проведении транзакций), «Восход» – за счет бюджета. При этом последний предложил два варианта: печатать карты на "Гознаке" либо на спецоборудовании в отделах полиции (это дороже на 8 млрд рублей). Кто именно будет разрабатывать защищенное мобильное приложение, неясно, если проект «Ростелекома» все же отклонили.

Новый УИК

Построение новой электронной системы оценивается, по предварительным расчетам, в 144 млрд рублей, эта сумма была заявлена в проекте «Цифровая экономика», деньги должны быть распределены до 2024 года. В сопоставимую сумму оценивался и предшественник проекта электронных паспортов – универсальная электронная карта (УЭК), единая идентификационная и платежная карта. На ее выпуск и внедрение планировалось потратить 135-165 млрд рублей, их начали выдавать в 2013 году, но позже проект свернули. В этом же году и была сформулирована концепция электронных паспортов.

Предполагалась, что выдавать их начнут в 2016 году, потом сроки перенесли на 2017-й и в итоге остановились на 2021-м. Причем осенью 2018 года карта с чипом описывалась с большим набором данных: паспорт, СНИЛС, права, отпечаток пальца и слепок лица, электронная подпись и код доступа к

цифровому профилю. Примечательно, что весной прошлого года тогда еще глава Центра стратегических разработок Алексей Кудрин предлагал реформу госуправления под лозунгом «Государство как платформа». В ней он описывал более радикальную концепцию электронных паспортов: создание «цифрового двойника» россиянина с авторизацией через биометрические данные, а также тотальную цифровизацию всего документооборота.

Государство, таким образом, разрабатывает, анонсирует и пытается внедрить электронные удостоверения личности последние 10 лет. За это время электронные удостоверения личности в разных форматах появились в нескольких странах. В Германии паспорта с чипом Personalausweis работают с 2010 года вместе с бумажными документами. В США электронным удостоверением личности с 2014 года выступают водительские права. В Китае третье поколение электронных карт вышло в обращение в 2001 году и сейчас проект ID-card уже прочно врос в экосистемы WeChat и Alipay. Однако самым ярким примером остается опыт соседней Эстонии, где ID-kaart с 2002 года выдаются всем гражданам по достижении 15 лет. На цифровизацию паспортов в этой стране ушло меньше 5 лет, но система периодически сталкивается со сбоями, самый масштабный произошел в 2017 году, когда из-за уязвимости чипов временно "заморозили" электронные удостоверения для половины страны.

Пилот и сбои

Опрошенные «ДП» участники рынка допускают запуск проекта в заданные сроки, но в пилотном режиме. Исходя из практики введения различных электронных документов — социальных карт, Карты москвича и петербуржца,

школьника и других проектов, сроки вполне реалистичны, даже несмотря на значительно большие масштабы проекта и объемы предстоящих работ, считает Дмитрий Буянов, GR-директор Group-IB. «Однако, чтобы с уверенностью утверждать это, необходим запуск пилотного проекта в городах-миллионниках, например, в Москве», — подчеркивает он.

О запуске пилотной зоны говорит и Андрей Янкин, директор центра информационной безопасности «Инфосистемы Джет», с оговоркой, что "масштабная перестройка работы бесчисленного количества государственных и бизнес-процессов, скорее всего, затянется на многие годы", а сроки могут сместиться из-за проблем с подделкой таких документов.

Более оптимистичен Павел Боровков, гендиректор консалтингового агентства «Партнеры и Боровков». «Наше государство показывает достаточно высокую эффективность в цифровизации тех сфер, которые ему действительно интересны. Наиболее яркий пример – это система сверки книг продаж и покупок плательщиков НДС. Неплохо работают единые базы судебной системы, выездов из РФ у погранслужбы, разные социально востребованные сервисы на "Госуслугах". Другое дело, что тестовый запуск не равен промышленной эксплуатации: однозначно, что первые опыты соберут массу недоработок, на ликвидацию которых уйдет не один месяц, а то и год», — поясняет эксперт.

Уже существуют действующий портал госуслуг, Единая система идентификации и аутентификации, есть опыт УИК, то есть разработано как нормативное регулирование аутентификации граждан и оказания услуг в электронном виде, так и часть необходимой инфраструктуры, подчеркивает

юрист практики по интеллектуальной собственности «Качкин и Партнеры» Андрей Алексейчук. Однако за установленный срок будет достаточно сложно изменить действующее нормативное регулирование и доработать по всей стране инфраструктуру, которая должна работать безотказно, подчеркивает юрист.

В «Техносерве» уверены, что заявленные сроки более чем реалистичны, с технологической точки зрения никаких проблем в производстве пластиковых карт с чипом и тем более в создании защищенного мобильного приложения нет. Главной угрозой в компании считают доступ к персональным данным. «Для минимизации ущерба во главе угла должна стоять информационная безопасность, а доступ к данным должен быть реализован через двухфакторную аутентификацию, в том числе с применением биометрической идентификации, например, “Единой биометрической системы”», – отметил Дмитрий Кульков, заместитель начальника управления отраслевой экспертизы Департамента по работе с госструктурами компании «Техносерв».

Сила бумаги и приватность

Ключевой проблемой для проекта может стать риск ошибочно внесенной информации, сбои системы, в результате которых информация может быть повреждена или утеряна, отмечают в «Доктор Веб». Кроме того, остается риск работы с мобильным приложением из-за небрежности к элементарным правилам цифровой гигиены. В «Лаборатории Касперского» уверены, что основной риск – это копирование и последующее клонирование электронной карты, но эта проблема актуальна, скорее, для бумажного

паспорта. «Другой вопрос, что основной массив личных данных хранится в электронных базах различных ведомств и утечки из подобных баз никак не связаны с типом паспортов», – пояснил Юрий Наместников, глава исследовательского центра компании.

Вадим Юсупов, коммерческий директор First Line Software, считает, что помимо технических проблем, сопутствующих такому проекту, важно учитывать и отставание законодательной базы от технического прогресса и обычное мошенничество. «Как пример можно привести появившиеся у нас факты мошенничества с введением электронно-цифровой подписи в практику сделок с недвижимостью и работы с налоговыми документами», – напоминает он.

Особенно это актуально на фоне новостей о постоянных утечках данных, в первую очередь из защищенного банковского сектора, напоминает эксперт «Качкин и партнеры». Кроме того, предполагается предоставление информации не только госорганам, но и коммерческим организациям, например, тем же банкам. «Соответственно, количество и категории лиц, которые имеют доступ к информации о гражданах, будет довольно большим и проконтролировать соблюдение требований к безопасности будет крайне проблематично», – считает Алексейчук, отмечая, что цифровые паспорта намерены внедрять в стране, где почти четверть населения по состоянию на конец 2018 года ни разу в своей жизни не подключалась к интернету.

«Мир – не только Россия – не готов к электронным документам, никто не научился хранить секретные данные», – возражает глава агентства PR Partner Инна Анисимова. «Америка имеет доступ ко всем передовым защитным

технологиям, но ее секретные электронные данные оказались уязвимы перед кучкой активистов из Wikileaks. Стоит ли говорить о том, что в России telegram-бот за 1 тыс. рублей продаст вам любую персональную информацию интересующего вас человека», – отмечает она.

Еще одним критическим фактором может стать вопрос приватности данных. Как отмечает Павел Боровков, паспорт – это часть более широкой концепции «Цифровой профиль гражданина», подразумевающей информирование государства обо всех аспектах жизни каждого человека. «Значит, если вы сторонник приватности информации о вашей жизни, электронные паспорта и цифровой профиль – это, конечно, угроза для таких ценностей», – уверен аналитик.

Проблема, скорее, не в создании системы, а в её внедрении в жизнь россиян, говорит **Светлана Немова, заместитель генерального директора ГК «КОРУС Консалтинг»**. Внедрение в заданные сроки возможно, по ее словам, в Петербурге, Москве, Казани. «В целом же перевод с бумажных паспортов во всей России кажется слишком оптимистичным. Даже в передовых по уровню цифровизации регионах можно столкнуться с неготовностью государственных и коммерческих сервисов к идентификации граждан по электронному паспорту. Не говоря уже про бабушек в деревнях без интернета – электронные паспорта они увидят ещё не скоро», - отмечает она.

Генеральный подрядчик

Все участники рынка единодушно признают, что разрабатывать и внедрять цифровые паспорта должен генеральный подрядчик, проверяемый на

каждом этапе независимыми аудиторami. Как подчеркивает Кирилл Солодовников, гендиректор Infosecurity (входит в Softline), проект должен быть максимально защищен на этапе запуска для дальнейшего поэтапного устранения уязвимостей.

В Group-IB уверены, что работающие на аутсорсе независимые эксперты в кибербезопасности должны привлекаться на самых ранних этапах. «При этом важно понимать, что на каждой стадии разработки (от пилота до тиражирования) необходимо привлекать не просто аудиторов защищенности систем и инфраструктурных компонентов ЭП, но и использовать RedTeaming, то есть комплекс работ по имитации атак на систему и ее отдельные звенья с целью выявления и ликвидации слабых мест», – подчеркивает Дмитрий Буянов.

Кроме того, исходные коды наиболее значимых программных компонентов, составляющих систему, должны быть раскрыты для изучения профессиональным IT-сообществом. Это достаточно распространенная практика в сфере информационных технологий, которая применяется в том числе крупнейшими IT-компаниями, например, Google, «Яндекс», Telegram, добавляет эксперт «Качкин и партнеры». В дальнейшей работе проекта также должны принимать участие экономически и юридически независимые компании-партнеры, поддерживающие работоспособность экосистемы, добавляет Боровков.

Предпочтительнее, чтобы разработкой и хранением занималась одна коммерческая организация, регулируемая ФСТЭК, работники которой будут нести уголовную ответственность за нарушение конфиденциальности,

целостности или доступности данных, обращает внимание **Сергей Прохоров, руководитель направления информационной безопасности департамента ИТ-аутсорсинга ГК «КОРУС Консалтинг»**. «При эксплуатации необходимо обеспечивать регулярный доступ по запросу авторизованных госорганов и организаций. Компании-разработчику гораздо проще в случае обнаружения проблем самостоятельно "закрывать дырки" в безопасности и реагировать на ухудшение производительности», – резюмирует он.

Источник: «Деловой Петербург»