

# СОВРЕМЕННЫЕ ВЫЗОВЫ ИНФОРМАТИЗАЦИИ И ПРАВООХРАНИТЕЛЬНАЯ ДЕЯТЕЛЬНОСТЬ

**И.В. Горошко**

*Институт проблем управления им. В.А. Трапезникова РАН*  
Россия, 117997, Москва, Профсоюзная ул., 65  
*Академия управления МВД России*  
Россия, 125171, Москва, ул. З. и А. Космодемьянских, 8  
E-mail: [garrygo@mail.ru](mailto:garrygo@mail.ru)

**Ю.В. Бондаренко**

*Воронежский государственный университет*  
Россия, 394018, Воронеж, Университетская пл., 1  
E-mail: [bond.julia@mail.ru](mailto:bond.julia@mail.ru)

**Ключевые слова:** большие данные, интернет вещей, искусственный интеллект, правоохранительная деятельность, управление.

**Аннотация:** Настоящая статья носит постановочный характер и является результатом некоторых размышлений авторов над вопросами, которые возникают в связи с поставленной грандиозной задачей построения в Российской Федерации информационного общества. Как решение данной задачи может отразиться на различных направлениях деятельности государства и, в частности, на деятельности правоохранительной? Какие изменения ждет данный вид деятельности, с какими рисками при его реализации можно столкнуться, внедряя цифровые технологии в общественные отношения? Обсуждению этих вопросов и посвящена настоящая статья.

## 1. Введение

Построение информационного общества, формирование цифровой экономики - были провозглашены стратегическими целями развития российского общества на ближайшее десятилетие. Глубинные трансформации, связанные с этими процессами, будут оказывать самое серьезное влияние как на систему государственного управления в целом, так и на отдельные ее элементы и направления деятельности.

Сегодня это влияние, как правило, предпочитают рассматривать в положительном аспекте. Действительно, внедрение искусственного интеллекта, интернет вещей, роботизация, виртуализация и т.п., призваны повысить эффективность управленческих процессов и поднять на новый уровень качество принимаемых решений.

Вместе с тем, как это часто бывает, масштабный характер настоящих и будущих преобразований затрудняет осознание потенциальных и реальных опасностей, которые скрывается за грядущими новациями. Особенно внимательно необходимо подойти к рассмотрению возможных последствий цифровизации общественных отношений для правоохранительной деятельности государства.

## 2. Цифровизация общества и правоохранительная деятельность

Широкомасштабное внедрение передовых информационных технологий является сегодня приоритетным трендом для большинства государств мира, включая и Россию. По оценкам специалистов объем инвестиций в новые технологии к 2020 г. достигнет 2,4 триллиона дол. [1]. Современные тенденции развития этих процессов достаточно красноречиво иллюстрирует лепестковая диаграмма прогнозируемой динамики совокупного среднегодового темпа роста инвестиций (CAGR) в различные направления цифровой экономики (рис.1).

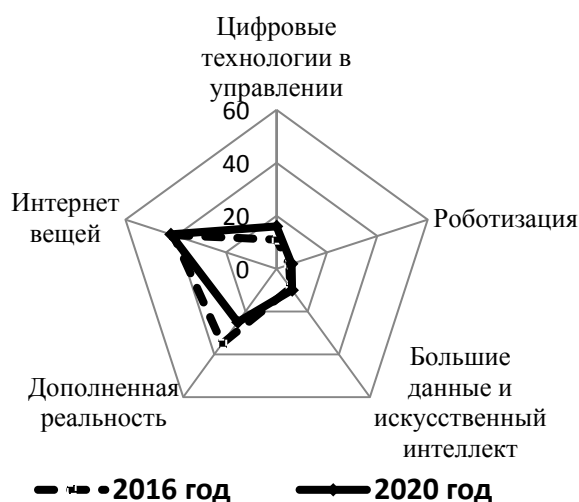


Рис.1. Динамика CAGR 2016-2020 гг.

Цифровизация общественных отношений затрагивает сегодня не только экономическую сферу, но и широкий спектр различных направлений государственной деятельности.

Правоохранительная деятельность является одним из важнейших видов государственной деятельности независимо от форм государственного устройства, правления или господствующего политического режима.

Она осуществляется специально уполномоченными органами, решающими задачи, связанными с обеспечением общественного порядка и общественной безопасности, раскрытием и расследование преступлений, охраной прав и свобод человека и гражданина.

В Российской Федерации к числу таких органов, как правило, относят прокуратуру, следственные органы, органы федеральной службы безопасности, органы внутренних дел.

Формируемая цифровая инфраструктура современного общества способна самым серьезным образом повлиять на выполнение правоохранительными органами правоохранительных функций.

Использование технологии блокчейн (распределенного управления конкурентным доступом) позволит обеспечить оперативный контроль за выполнением решений, принимаемых в правоохранительной деятельности и высокий уровень доверия к ним, который обеспечивается прозрачностью сетевых транзакций.

Обработка «больших данных» может стать основой для повышения эффективности охраны общественного порядка и общественной безопасности, помогая прогнозировать преступность, автоматически отслеживать большие скопления людей, зоны риска, аномальную активность геотегинга, анализировать банки данных оперативно-разыскной, статистической, криминалистической информации (в том числе генетической), социальные сети. Опыт многих компаний, использующих качественную аналитику данных как фактор роста, доказывает этот тезис.

Технологии искусственного интеллекта, применяемые при производстве различного рода роботов, автономных транспортных средств, в системах компьютерного зрения, обработки естественного языка, хорошо адаптируются для потребностей правоохранительной деятельности, например они востребованы при выработке рекомендаций в процессе принятия управленческих решений, расследовании конкретных преступлений и т.п.

Проведенный Всемирным банком анализ присутствия в человеческой жизни интернет вещей свидетельствует о том, что во многих государствах все активнее используются подключенные к интернету устройства для решения стратегических и текущих задач городского строительства [2]. Представляется возможным применять эти устройства и в целях совершенствования деятельности патрульно-постовой службы, управления городским транспортом, обеспечения безопасности дорожного движения.

Предполагается, что в недалеком будущем к объектам реального мира будут подсоединены более 20 млрд. датчиков, что позволит создать в виртуальном мире цифровые двойники для миллиардов существ [3]. В результате конкретные физические лица или технические объекты будут заменены их точными цифровыми отображениями, которые могут быть использованы для моделирования и прогнозирования поведения людей как в обычных, так и в чрезвычайных ситуациях.

Вышеперечисленные примеры демонстрируют те возможности, которые предоставляют современные информационные технологии для совершенствования правоохранительной деятельности.

Вместе с тем процессы цифровизации несут в себе и определенные вызовы, формируют повышенные требования к адаптивным способностям государства.

Прежде всего, они способны привести к пересмотру веками сложившихся подходов к построению системы государственного управления, механизмов государственного контроля и надзора.

Демократичная технология блогчейна, с ее открытостью и полным равноправием участников, предполагает децентрализацию управления, в том числе и в правоохранительной сфере. Государство при таком подходе минимизирует свои функции регулятора и само находится под пристальным контролем многочисленных оппонентов.

Глобальная информатизация, распространение технологий, способствующих росту информационной открытости существенно повысили уязвимость государственных структур и привели к появлению альтернативных центров власти – центров, основные усилия которых направлены на формирование благоприятного им информационного фона. Примером этому служат истории с Джулианом П. Ассанжем и WikiLeaks, движением Anonymus и TYLER и т.п.

Игнорирование этих фактов неизбежно приведет к поляризации и радикализации общественного мнения, что повысит нагрузку на правоохранительные органы.

Использование современных алгоритмов, обрабатывающих «большие данные», технологий искусственного интеллекта позволяют обеспечить идентификацию личности по косвенным признакам, например по одной фотографии, взятой с камер наружного наблюдения. По сути, речь идет о возможности беспрепятственно установить персо-

нальные данные конкретного лица без его согласия. Потеря приватности открывает дорогу новым, еще не известным ранее формам дискриминации личности.

Кроме того, в формируемом глобальном информационном пространстве под угрозой окажутся аккаунты в социальных сетях, электронные почтовые ящики, банковские карты, карты медицинского страхования. Это неизбежно приведет к появлению новых способов мошенничества и увеличению размеров наносимого ущерба. Уже сегодня рынок преступлений в области интернет-банкинга превышает 10 млрд. руб., а количество «утекших» записей персональных данных из коммерческих компаний и государственных организаций исчисляется в миллиардах.

Для того, чтобы справиться с этими вызовами, правоохранительным органам цифрового будущего необходимо будет перейти на новый качественный уровень, где современные информационные технологии станут неотъемлемой частью правоохранительной деятельности.

### 3. Заключение

В заключении подчеркнем, что мы рассмотрели лишь незначительную часть проблемных вопросов, которые могут возникнуть при реализации проекта построения информационного общества в России. Задавая эти вопросы сейчас, на первых шагах перехода от электронного к умному управлению, мы тем самым готовимся сформулировать возможные предложения по профилактике отрицательного влияния цифровизации общественных отношений на правоохранительную деятельность. Представляется, что обоснование подобных предложений может стать целью самостоятельной научной проработки.

### Список литературы

1. <http://reports.weforum.org/digital-transformation/wp-content/blogs.dir/94/mp/files/pages/files/dti-executive-summary-20180510.pdf>
2. Lal Das P., Beisswenger S.C., Mangalam S., Yuce M.R., Lukac M. Internet of things: the new government to business platform - a review of opportunities, practices, and challenges. Washington: World Bank Group, 2017. С. 112-114. //URL: <http://documents.worldbank.org/curated/en/610081509689089303/Internet-of-things-the-new-government-to-business-platform-a-review-of-opportunities-practices-and-challenges>
3. Desjardins J. How the Internet of Things has evolved over the last 50 years // URL: <https://www.weforum.org/agenda/2018/01/how-the-internet-of-things-has-evolved-over-the-last-50-years>