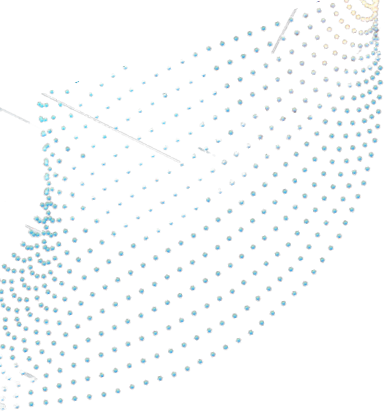
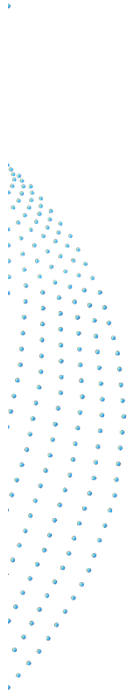
Цифровая трансформация государственного управления: Кейсы и лучшие практики





Оглавление

Введение

Цифровая трансформация – один из основных приоритетов современной экономики. Данный процесс включает не только внедрение новых технологий и технологических решений в повседневную жизнь компаний и организаций, но и переход к новым практикам и возможностям для управления, распределения ответственности и полномочий, а также взаимодействия с внешними контрагентами. По различным подсчетам объем только частных инвестиций в цифровую трансформацию составит от 2,4 до 2,8 трлн долл. США к 2023 г. Общие же расходы на информационную инфраструктуру и информационные технологии (ИТ) достигнут 4,6 трлн долл. США к 2023 г. Кроме того, ожидается, что к 2023 г. более половины мирового ВВП будет произведено компаниями и организациями, прошедшими цифровую трансформацию.

Для государственного сектора цифровая трансформация также является ключевым приоритетом по ряду причин:

1. Усложнение экономических, социальных, политических, демографических и иных процессов требует как новых подходов к государственному управлению, так и новых методов и технологий анализа и обработки информации, формирования стратегического видения и определения приоритетов;
2. Цифровизация улучшает качество государственного управления и доступность предоставляемых населению государственных услуг. Кроме того, цифровизация государственных органов открывает возможности для появления новых видов услуг для населения;
3. Цифровизация повышает прозрачность процесса принятия решений государственными органами, что в свою очередь усиливает подотчетность и целостность госуправления;
4. В условиях кризисов, в частности, пандемии COVID-19, экологических, социальных и геополитических рисков, цифровизация повышает возможности государственного сектора по принятию своевременных и обоснованных решений.

По некоторым оценкам глобальный экономический эффект от цифровой трансформации органов государственного управления может достигать 1 трлн долл. США в год.

Эволюция концепции цифрового правительства

Организации государственного сектора все чаще используют информационные технологии для повышения качества, оперативности и прозрачности предоставления государственных услуг. Процесс цифровой трансформации госсектора начался задолго до пандемии COVID-19, однако именно необходимость массовой удаленной работы сотрудников в условиях локдаунов показала эффективность перевода процессов в цифровой формат.

Нельзя сказать, что процессы цифровой трансформации носят поступательный характер. По данным экспертов Deloitte, полученным в 2015 г. в ходе опросов представителей органов государственной власти 70 стран мира, показывают, что до 75% респондентов настороженно относятся к процессам трансформации, полагая, что они во многом подрывают сложившийся привычный порядок работы. В то же время цифровая трансформация воспринимается в качестве неизбежного процесса.

Цифровая трансформация в государственном и частном секторах

Процессы цифровой трансформации в частном и государственном секторах во многом схожи и заключаются в постепенном переходе цифровых технологий из инструмента в основной драйвер стратегического развития. Однако в отличие от бизнеса цифровизация госуправления должна соответствовать ряду ключевых условий:

- **Универсальность государственных услуг.** Частный сектор ориентирует или адаптирует свои продукты и услуги под определенные запросы групп населения. В свою очередь, государственные услуги предназначены для использования всеми без исключения гражданами и должны отвечать потребностям всего населения, а также быть удобными в получении.
- **Более широкий набор сфер применения**. В отличие от частного сектора, государство предоставляет услуги практически во всех сферах, частично выступая конкурентом частного сектора, и в то же время является поставщиком услуг в тех отраслях, которые недоступны частным компаниями.
- **Больше критериев оценки успешности цифровизации**. В отличие от частных компаний, успешность которых измеряется категориями «издержек-выгод», набор критериев эффективности для госуслуг включает не только удовлетворенность граждан предоставляемыми услугами, доступность этих услуг и т.д., но и соответствие стратегическим целям национального развития, которые, как и предпочтения граждан, могут меняться в зависимости от политической конъюнктуры.
- **Высокие требования к надежности и безопасности**. Помимо изначально высоких требований к надежности, качеству, доступности и эффективности предоставление государственных

услуг является объектом пристального внимания представительных органов законодательной власти и высших органов аудита (ВОА).

Кроме того, непосредственный процесс цифровой трансформации органов государственной власти практически всегда сталкивается с рядом наиболее характерных вызовов:

- **Ограниченные бюджеты** на цифровую трансформацию, в особенности на критически важные технологии и решения;
- **Строгие правила** и процедуры регулирования использования данных препятствуют быстрому внедрению новейших технологий;
- Основной приоритет в разработке продуктов и технологий – **вопросы кибербезопасности**, а не удобство пользования и повышение эффективности;
- **Невозможность успешной цифровизации** отдельных органов госуправления – для успешного взаимодействия и слаженной работы требуется цифровизация всего госсектора на основе единых или схожих решений и платформ;
- **Выраженный «разрыв поколений»** между руководством и сотрудниками органов государственной власти в условиях централизованного принятия решений в значительной степени препятствует быстрой цифровизации госуправления. Цифровая трансформация государственных органов требует предварительной просветительской и технологической работы по развитию восприимчивого внутреннего рынка и сокращению «цифровых разрывов» (digital divides).

В результате реализация ключевых компонентов цифровой трансформации госструктур сильно зависит от политической воли руководства, выраженной в национальных стратегических и программных документах.

Ключевые компоненты перехода правительства на цифровые технологии

1. **Видение, лидерство, мировоззрение**: Укрепление трансформационного лидерства, изменение мировоззрения и цифровых возможностей на индивидуальном уровне
2. **Институциональная и нормативная база**: Развитие нормативно-правовой и организационной экосистем как по горизонтали, во всех секторах экономики на национальном, региональном и муниципальном уровнях, так и по вертикали, во всех структурах государственного управления, производства и услуг
3. **Системное мышление и интеграция:** содействие комплексным подходам к разработке политики и предоставлению услуг
4. **Управление данными:** Обеспечение стратегического и профессионального управления данными для реализации фактологически подкрепленных политических решений
5. **Инфраструктура ИКТ, доступность технологий**
6. **Ресурсы**: Мобилизация ресурсов и согласование приоритетов, планов и бюджетов; в том числе на основе партнерских отношений между государственным и частным секторами
7. **Развитие цифровых навыков и подготовка высококвалифицированной рабочей силы**
8. **Общественный потенциал**: Расширение социального охвата цифровых услуг и использование ИКТ для снижения общественного неравенства

Отсутствие конкуренции как драйвера инноваций госорганы способны компенсировать возможностью самостоятельно задавать стандарты реформ. Так, по оценкам Всемирного банка в крупных странах с развивающейся экономикой цифровая трансформация государственного сектора значительно опережает аналогичные показатели частного сектора.

Процесс цифровизации государственного управления

Формирование цифрового правительства – эволюционный процесс, включающий несколько этапов развития.

Источник: Всемирный Банк (GovTech Maturity Index: The State of Public Sector Digital Transformation, 2021)

Электронное правительство (E-government) — использование информационных технологий для автоматизации рабочих процессов, повышения эффективности управления данными, улучшения качества предоставления государственных услуг, развития каналов коммуникаций. В рамках электронного правительства существуют три типа взаимодействия: отношения между государственными институтами (G2G); отношения по линии «правительство-бизнес» (G2B) и взаимодействие правительства с гражданами (G2C).

Модель развития электронного правительства ООН

Этап 1	Онлайн-публикация государственной информации
Этап 2	Предоставление расширенной информации о деятельности госорганов, взаимодействие между правительством и гражданами посредством использования загруженных на портал электронных форм
Этап 3	Двустороннее интерактивное взаимодействие между правительством и гражданами, постепенное вовлечение граждан в процесс государственного управления при помощи информационных технологий (электронное голосование, заполнение налоговых деклараций, а также заявки на получение лицензий, осуществление финансовых транзакций)
Этап 4	Координация процессов внутри и между государственными учреждениями на основе цифровых решений, полноценное цифровое участие граждан в процессе госуправления

Цифровое правительство (Digital Government) развивает концепцию электронного правительства, использует оцифрованные данные для проактивного предоставления социально ориентированных государственных услуг.

Выделяют шесть основных компонентов цифрового правительства:

- цифровая **инфраструктура**;
- цифровая **грамотность**;
- цифровые **коммуникации**;
- активное **использование** информационных технологий;
- нормативное **регулирование** цифровой среды;
- информационная **безопасность** и цифровые права.

Среди ключевых элементов цифровой архитектуры правительства – единый государственный информационный портал, система совместного управления данными из реестров разных государственных структур; предоставление госуслуг в формате «одного окна»; открытая база цифровых решений, инновационные системы сбора и анализа данных, обеспечение кибербезопасности и надежной защиты персональной информации.

Согласно методологии Всемирного банка, в качестве критериев оценки эффективности цифровой трансформации выделяют:

- **время** предоставления услуги;
- **популярность** цифровых каналов взаимодействия с государством;
- **качество** перевода государственных услуг в цифровой формат;
- **количество** автоматически обработанных запросов;
- **уровень** цифровой грамотности населения;
- **сокращение** финансовых затрат;

- **сокращение** случаев мошенничества и коррупции.

Приоритетными направлениями повышения цифровой зрелости правительства и государственных органов также являются:

- **агрегирование** и **систематизация** разрозненных данных в целях повышения эффективности оказания государственных услуг;
- **создание** безопасной и гибкой технологической инфраструктуры;
- **повышение** профессионального потенциала, проведение кадровой политики с акцентом на цифровые компетенции;
- **взаимодействие** с представителями научного и бизнес-сообщества для обмена лучшими практиками в области цифровизации и инноваций;
- периодическая **оптимизация** рабочих процессов, максимальное использование трудового и технологического потенциала;
- **развитие** цифровой экосистемы в соответствии с потребностями пользователей государственных сервисов.

Организация Объединенных Наций (ООН)

По оценкам ООН, среднемировой показатель Индекса развития электронного правительства (e-Government Development Index, EGDI) продолжает расти, достигнув 0,6 в 2020 г. по сравнению с 0,55 в 2018 г. Согласно результатам исследования за 2020 г., 36% (69) составляют государства с высокими показателями EGDI, 31% (59) – государства со средними показателями EGDI, 29% (57) – страны с очень высокими показателями EGDI, 4% (8) – страны с низкими показателями EGDI (доля с 8% до 4 % с 2018 по 2020 гг.)

Индекс развития электронного правительства ООН публикуется Департаментом Организации Объединенных Наций по экономическим и социальным вопросам (ДЭСВ ООН) каждые два года, начиная с 2001 г. Оценка проводится для всех 193 стран – членов организации. В состав сводного индекса включены три индикатора:

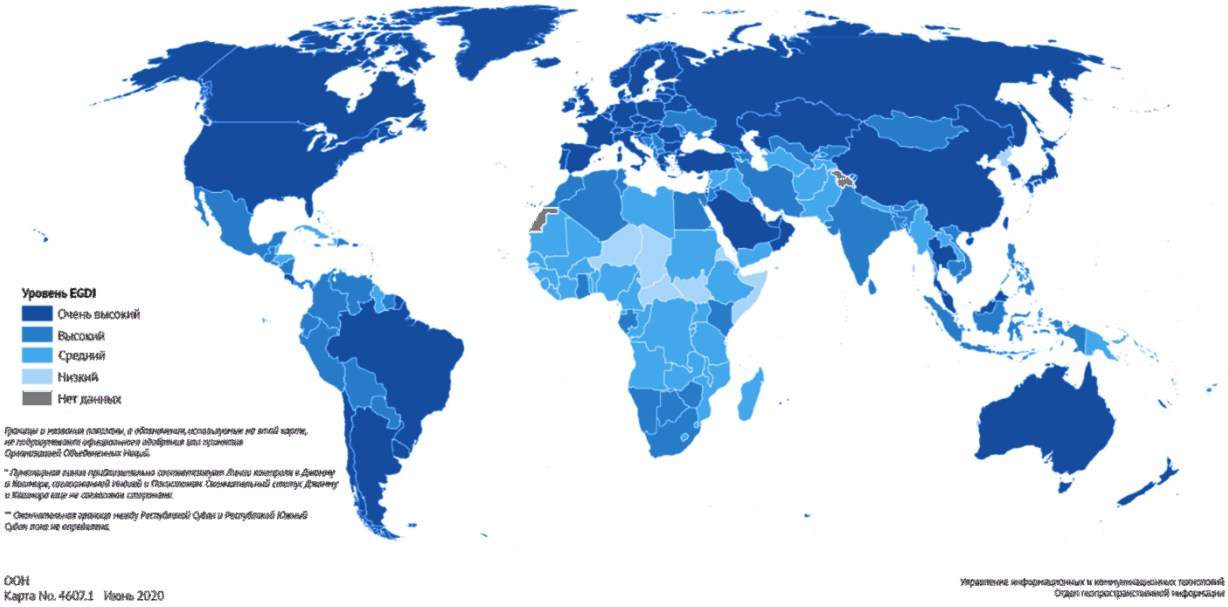
- индекс **телекоммуникационной инфраструктуры** (TII), основанный на данных Международного союза электросвязи (МСЭ);
- индекс **человеческого капитала** (HCI), основанный на данных ЮНЕСКО;
- индекс **онлайн-услуг** (OSI), основанный на данных социологического опроса ДЭСВ.

По итогам оценки страны делятся на 4 категории: страны с очень высоким показателем EGDI (0,75 – 1), высоким показателем EGDI (0,5 – 0,75), средним показателем EGDI (0,25 – 0,5), низким показателем EGDI (0 – 0,25).

Более 80% государств – членов ООН переводят государственные услуги для граждан в цифровой формат. Наиболее распространенными цифровыми сервисами являются: регистрация нового бизнеса, получение свидетельства о рождении и смерти, оформление разрешения на строительство, оплата коммунальных услуг. 95% стран имеют государственный онлайн-портал с базовыми функциями поиска и обратной связи.

Руководствуясь принципами ЦУР 16 по повышению прозрачности и подотчетности государственных институтов, правительства активно используют цифровые платформы для организации процесса государственных закупок и трудоустройства. С 2018 г. число стран, публикующих открытые вакансии в Интернете, увеличилось на 30%. Более 70% (138 стран) публикуют результаты закупок/торгов онлайн, 65% (125) имеют специализированные платформы электронных закупок.

Географическое распределение четырех групп EGDI, 2020 г.



Источник: «Исследование ООН: Электронное правительство 2020»

Среди лидеров по развитию цифрового правительства – Австралия, Великобритания, Дания, Исландия, Республика Корея, Нидерланды, Новая Зеландия, Норвегия, Сингапур, Соединенные Штаты Америки, Финляндия, Швеция, Эстония и Япония. Россия занимает 39 место (0,8176) и входит в группу стран с очень высоким показателем электронного участия.

Несмотря на достигнутый прогресс, эксперты ООН констатируют наличие цифрового разрыва как внутри регионов, так и между ними. Ограниченность финансовых ресурсов, отсутствие инфраструктуры и стратегии цифровой трансформации госуправления, а также низкий профессиональный уровень ответственных лиц и стейкхолдеров – ключевые факторы, сдерживающие цифровое развитие в развивающихся странах.

Цифровая трансформация госуправления требует новых подходов, отличающихся от инициатив по созданию электронного правительства. Приоритетами цифровой трансформации в современных условиях являются: внедрение платформенных решений, использование технологий искусственного интеллекта (ИИ) и блокчейна, повышение цифровой зрелости населения, оказание цифровых услуг на основе инструментов анализа данных.

Цифровое правительство открыто и доступно для участия всех заинтересованных сторон. Цифровые платформы используются не только для информирования, но и для привлечения граждан к процессу принятия решений и преодоления бюрократических барьеров в межведомственном взаимодействии.

Индекс электронного участия ООН (E-participation index, EPART) включает оценку трех компонентов:

- **электронное информирование**: обеспечение участия путем предоставления гражданам государственной информации и доступа к информации по требованию или без;
- **электронные слушания**: вовлечение граждан в обсуждения и принятие решений по вопросам государственной политики и услуг;
- **электронное принятие решений**: предоставление гражданам возможности принимать непосредственное участие в принятии решений.

С 2016 г. оцениваемые страны относят к одной из четырех групп на основе их соответствующих значений EPI: страны с низким уровнем EPI (0 – 0,25), со средним уровнем EPI (0,25 – 0,5), с высоким уровнем EPI (0,5 – 0,75), с очень высоким уровнем EPI (0,75 – 1). Страны с наивысшим индексом электронного участия в 2020 г. – Австрия, Великобритания, Республика Корея, Эстония, Новая Зеландия, Сингапур, США, Япония.

Результаты исследования 2020 г. свидетельствуют о росте количества правительственных порталов с функциями обратной связи, голосования и комментирования. Однако многие страны по-прежнему не располагают цифровыми ресурсами для предоставления инклюзивных услуг и привлечения граждан к участию в госуправлении.

Организация экономического сотрудничества и развития (ОЭСР)

Повышение эффективности и прозрачности деятельности государственного сектора стало возможным благодаря внедрению информационных технологий и переводу государственных услуг в электронный формат. Следующий шаг – использовать цифровые технологии для создания более открытых, инклюзивных и сетевых моделей государственного управления, а также формирования культуры принятия решений, основанных на данных.

Рекомендации ОЭСР по разработке государственной стратегии цифровой трансформации

Источник: ОЭСР, OECD Recommendation of the Council on Digital Government Strategies

Эксперты ОЭСР выделяют 6 ключевых характеристик цифрового правительства:

- **цифровизация** всего процесса принятия решений;
- **аналитика** данных как основа принятия политических решений;
- правительство как **платформа** (формирование единой цифровой экосистемы);
- **открытое** правительство;
- государственная политика в соответствии с **потребностями** граждан;
- **проактивное** предоставление госуслуг.

В справочном Руководстве ОЭСР по управлению цифровым правительством (The E-Leaders Handbook on the Governance of Digital Government) представлены рекомендации по осуществлению цифровой трансформации и повышению цифровой зрелости госсектора, разработанные на основе опыта стран-членов и стран – партнеров организации.

В Руководстве определены три основных фактора, которые необходимо учитывать при разработке и реализации цифровых проектов.

- **Контекстуальные факторы (Contextual Factors).** Необходимо определять принципы и механизмы управления проектами в соответствии с политическими, социально-экономическими, технологическими, географическими особенностями страны.
- **Институциональные модели (Institutional Models).** Решающее значение для устойчивой и эффективной цифровизации государственного сектора имеет открытость, прозрачность, упорядоченность и согласованность организационно-управленческих процессов.
- **Политические рычаги (Policy Levers)** – жесткие или мягкие инструменты, которые политическое руководство использует для поддержки рациональной и согласованной реализации стратегии цифровой трансформации, включая стратегическое планирование, механизмы финансового управления, нормативно-правовое регулирование и стандартизацию.

Всемирный банк (ВБ). Индекс зрелости GovTech

ГосТех (GovTech) – цифровой подход к модернизации государственного сектора, к оторый способен улучшить качество предоставления государственных услуг, упростить взаимодействие с гражданским обществом, повысить эффективность государственного управления. Под понятием ГосТех может подразумеваться целый ряд самых разных направлений деятельности: от формирования «умной» городской среды до применения цифровых инструментов для борьбы с преступностью.

ГосТех опирается на четыре основных элемента:

- **внедрение** цифровых платформ на основе аналитики больших данных;
- **развитие** общедоступных, клиентоцентричных цифровых сервисов;
- прямое мультиканальное **взаимодействие** государства и граждан;
- создание правовых и организационных условий для внедрения инноваций в госсекторе.

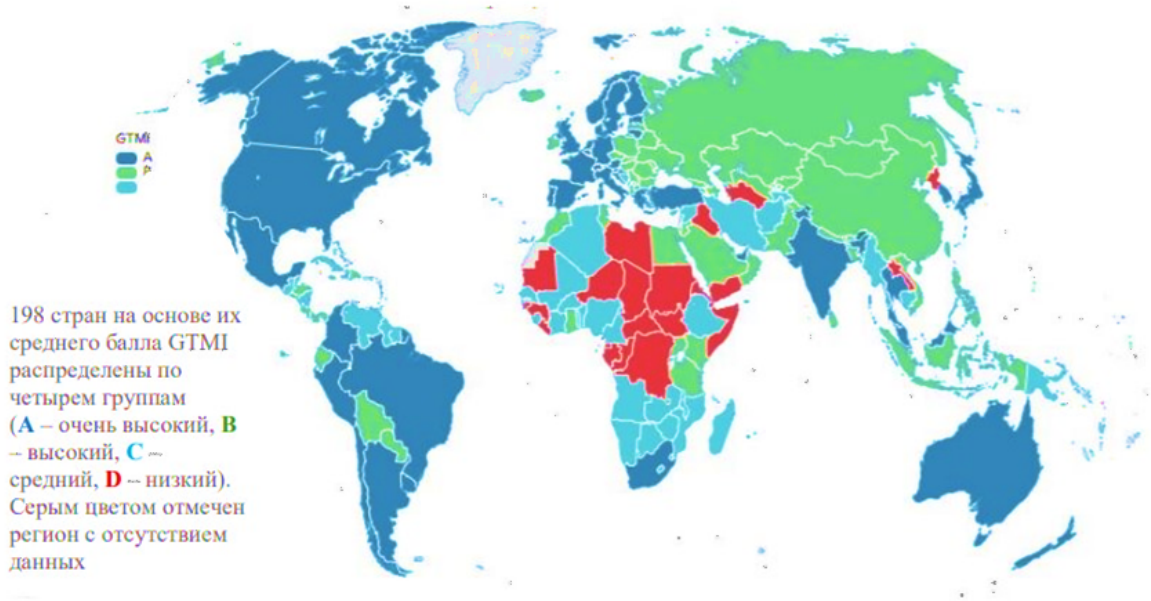
В практическом плане ГосТех представляет собой совокупность направлений деятельности, ориентированных на повышение эффективности государственного управления и процессов в четырех основных категориях:

- **Цифровое правительство.** Сюда относятся, в частности, платформы для принятия решений, цифровая идентификация, электронное голосование, G2G и G2B-услуги (электронные налоги, банкинг и др).
- **Умный город**: городское плани рование, управление отходами, транспортные системы и системы мониторинга, решения по энергосбережению.
- **CrimeTech**: системы распознавания личности, решения в области кибербезопасности, электронные суды, цифровые инициативы по противодействию отмыванию денег.
- **Государственное управление**: образовательные платформы, системы здравоохранения, решения в области спорта и развлечений, агротехнологии.

ГосТех обладает огромным потенциалом, однако превращение цифровых инициатив в осязаемые, измеримые и последовательные результаты в большинстве стран остается сложной задачей. Движение в сторону ГосТеха требует единого общегосударственного подхода к цифровой трансформации, создания прозрачной системы управления и принятия решений, использования потенциала государственно-частного партнерства для привлечения компетенций, инноваций и инвестиций частного сектора.

Для оценки степени «зрелости» ГосТеха эксперты Всемирного банка разработали «Индекс зрелости GovTech: состояние цифровой трансформации государственного сектора» (GovTech Maturity Index (GTMI): The State of Public Sector Digital Transformation). Индекс основан на оценке результатов цифровой трансформации в 198 странах мира. Кроме того, доклад включает обзор лучших практик использования цифровых инструментов в государственном секторе.

По результатам исследования, в 43-х странах цифровая трансформация занимает важнейшее место в стратегической повестке государства, а также отмечается успешная реализация многочисленных инновационных проектов. Среди лидеров цифровой трансформации – Австралия, Австрия, Индия, ОАЭ, Республика Корея, Сингапур, Швейцария, ЮАР. При этом в 33 странах наблюдается минимальное внимание к инициативам в сфере ГосТех. Цифровой разрыв наиболее заметен в странах Африки к югу от Сахары и Южной Азии.



Источник: «Индекс зрелости GovTech: состояние цифровой трансформации государственного сектора» (GovTech Maturity Index (GTMI): The State of Public Sector Digital Transformation)

Несмотря на увеличение инвестиций в цифровую инфраструктуру и активную разработку государственных программных документов в этой области, цифровая зрелость в большинстве стран остается на недостаточном уровне: 47% стран не имеют стратегий по развитию цифровых навыков среди населения.

Основными барьерами остаются:

- **отсутствие** политической воли государственного руководства и соответствующего нормативного регулирования;
- **неразвитая** цифровая инфраструктура;
- **низкий уровень** цифровой грамотности населения, а также государственных служащих;
- **неэффективное** или недостаточное финансирование.

Для повышения цифровой зрелости и адаптации к новой «нормальности» эксперты ВБ рекомендуют провести ревизию государственных подходов к цифровой трансформации: сосредоточиться на улучшении совместимости существующих информационных систем, создании многофункциональных платформ, формировании культуры эффективного управления большими данными, развитии необходимых цифровых навыков у населения.

Цифровая инфраструктура

Цифровая трансформация государственного управления невозможна без развития соответствующей информационно-коммуникационной или цифровой инфраструктуры. Развитие цифровой инфраструктуры обеспечивает не только функционирование государственных цифровых сервисов, но и непрерывную связь с основными пользователями и потребителями услуг, а также оперативный сбор и анализ необходимых данных. Кроме того, непрерывное совершенствование и развитие цифровой инфраструктуры позволяет своевременно адаптировать систему государственного управления и правительственные сервисы под потребности граждан. Наконец, развитие цифровых сервисов и инфраструктуры повышает прозрачность и подотчетность государственного управления, тем самым способствуя устойчивому развитию государственного управления.

К цифровой инфраструктуре относят:

- физическое оборудование;
- программное обеспечение;
- производственные помещения и здания, где располагается соответствующая инфраструктура;
- информационные сети;
- серверы;
- дата-центры.

Также в рамках цифровой инфраструктуре выделяют:

- **традиционную** инфраструктуру (включает все вышеперечисленное);
- **облачную** инфраструктуру (допускает удаленное использование компонентов инфраструктуры).

IT-инфраструктура является одним из основных компонентов затрат на цифровизацию госуправления. Общие затраты правительств стран мира на цифровую инфраструктуру превысили 500 млрд долл. США в 2021 г. Несмотря на некоторое снижение годовых темпов роста затрат на развитие цифровой инфраструктуры, ожидается, что по итогам 2022 г. общие затраты правительств на цифровую инфраструктуру вырастут до 557 млрд долл. США.

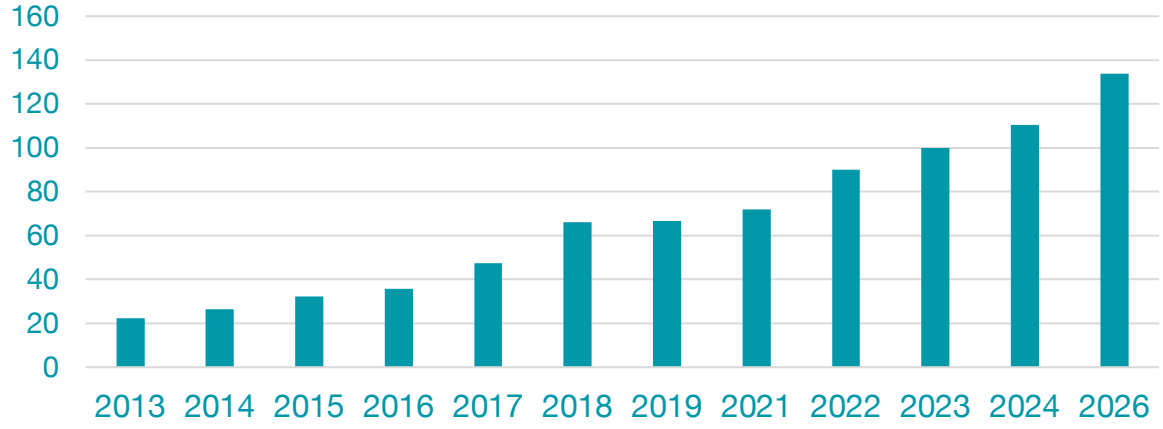
Общие расходы правительств стран мира на IT-инфраструктуру по секторам, 2021-2022 гг. (в млн долл. США)

Сектор	2021	Динамика роста к предыдущему году (в %)	2022	Динамика роста к предыдущему году (в %)
Цифровые услуги	188,069	10,9	203,922	8,4
Программное обеспечение	135,630	14,9	151,885	12,0
Услуги связи	61,482	1,4	60,996	-0,8
Внутренняя связь	64,245	0,3	65,971	2,7
Устройства	41,049	17,6	40,390	-1,6
Дата-центры	32,735	6,5	34,154	4,3
Общие расходы	523,212	9,5	557,318	6,5

Источник: Gartner, 2021, https://www.gartner.com/en/newsroom/press-releases/2021-08-31-gartner-forecasts-global-government-it-to-grow-in-20220

Помимо тренда на рост расходов на цифровую инфраструктуру в целом наблюдается рост инвестиций правительств в облачные сервисы. Это вызвано в том числе общим ростом числа и популярности облачных сервисов, а также возможностью оптимизации расходов по сравнению с традиционным подходом к цифровой инфраструктуре.

Мировые расходы на облачную IT-инфраструктуру в млрд долл. США



Источник: Statista, https://www.statista.com/statistics/503686/worldwide-cloud-it-infrastructure-market-spending

В то же время, несмотря на рост расходов на IT-инфраструктуру, именно данная сфера наиболее часто сталкивается с рядом серьезных проблем. В частности, общие проблемы развития цифровой инфраструктуры большинства стран зачастую сводятся к следующим аспектам:

- **нехватка** финансирования (скорость развития и обновления технологий и технологических решений опережает темпы роста расходов на цифровую инфраструктуру);
- **недостаток** квалификации и навыков сотрудников (до 40% организаций госсектора сталкиваются с нехваткой цифровых знаний и навыков у сотрудников);
- **низкая** степень интеграции цифровых систем и платформ внутри и между госорганами;
- наличие и необходимость поддержания работы **устаревших** систем (legacy systems);
- **низкий** уровень доверия граждан (граждане опасаются доверять свои персональные данные госорганам).

Кейсы

ВОА	**Национальное контрольно-ревизионное управление Великобритании (UK National Audit Office)**
Название	**Национальная система сбора и обработки данных в сфере правоохранительной деятельности (National Law Enforcement Data Programme)**
Дата	**10/09/2021**
Ссылка	

Национальное контрольно-ревизионное управление Великобритании (ВОА Великобритании) провело аудит программы создания Национальной системы сбора и обработки данных в сфере правоохранительной деятельности. Программа, осуществлявшаяся под руководством Министерства внутренних дел, была нацелена на создание единой базы данных и информационного сервиса вместо ранее существовавших 2 независимых сервисов полиции. Вместе с тем, по мнению ВОА программа столкнулась с серьезными проблемами, в частности в вопросах изначальной постановки технического задания (что привело к перезапуску процесса создания нового сервиса), а также увеличению расходов. По мнению ВОА, текущие результаты стоит признать неудовлетворительными, поскольку в условиях отсутствия нового сервиса и проблем с поддержкой старых это привело к существенным проблемам для конечных пользователей.

В рамках дальнейшей работы по развитию и внедрения системы, ВОА Великобритании рекомендует обратить внимание на следующие вопросы:

1. Провести повторную оценку проекта с учетом основных требований стейкхолдеров и финансовых затрат на всем цикле реализации;
2. Разработать стратегию постепенного перехода на новую информационную систему с учетом рисков срыва сроков и необходимости устранения ошибок и недоработок;
3. Проводить регулярную оценку технических возможностей системы, а также навыков и компетенций сотрудников;
4. При осуществлении закупок по государственному контракту на разработку системы у разных поставщиков обеспечить координацию из единого центра (МВД) на основе анализа рисков и заинтересованности участвующих сторон

ВОА	**Счетная палата ФРГ (Bundesrechnungshof)**
Название	**Стратегическое управление проектами в сфере цифровизации федеральных органов власти в Германии (Strategic management of digitalization projects in federal agencies of Germany)**
Дата	**27/07/2022**
Ссылка	

Счетная палата ФРГ (ВОА ФРГ) провела ряд проверок по вопросам реализации Цифровой стратегии (Digitalisation Strategy) в федеральных государственных органах. В рамках аудита ВОА изучил меры федерального правительства по достижению целей Цифровой стратегии, а также соответствующие действия Федерального министерства по делам цифровизации и транспорта (Bundesministerium für Digitales und Verkehr).

ВОА выявил, что федеральные ведомства не согласовали свои стратегии в области цифровизации с программными документами ФРГ. В некоторых случаях аудиторы выявили полное отсутствие ведомственной стратегии, в отдельных ведомствах цифровые проекты реализовывались исключительно в рамках конкретного подразделения, а не всего ведомства.

Кроме того, федеральные ведомства некорректно оценили приоритетность цифрового развития в своей деятельности, нецелесообразно определив цели и сроки реализации проектов. В результате на цели цифровизации было выделено недостаточное количество финансовых и кадровых ресурсов. Также в стратегическое управление цифровыми проектами не был вовлечен специально созданный в данных целях межведомственный комитет, что привело к значительному снижению согласованности цифровых стратегий ведомств.

ВОА рекомендовал ведомствам разработать собственные стратегии цифрового развития, согласованные с федеральными программными документами. Также ВОА позитивно оценил планы федерального правительства по пересмотру Цифровой стратегии и рекомендовал Федеральному министерству по делам цифровизации и транспорта активно взаимодействовать с ведомствами по цифровым проектам.

ВОА	**Управление Генерального аудитора Дании (Auditor General Office of Denmark)**
Название	**Отчет об использовании преимуществ государственных ИТ-проектов (Report on management of benefits in government IT projects)**
Дата	**17/09/2020**
Ссылка	

ВОА Дании провел аудит использования правительством и органами государственной власти преимуществ от внедрения IT-проектов, систем и инфраструктуры. По мнению аудиторов, несмотря на значительные усилия по цифровизации процессов и проектов, органы государственной власти не в полной мере используют полученные от реализации IT-проектов преимущества.

Среди возможных причин неэффективного использования цифровых инструментов и проектов аудиторы выделяют следующие:

1. министерства не ведут строгий и системный контроль и учет реализации цифровых проектов, а также возможных преимуществ использования цифровых систем;
2. вследствие отсутствия системных мер контроля полученных преимуществ, многие из них не реализуются в полной мере.

ВОА	**Государственное управление аудита Республики Латвия (The State Audit Office of the Republic of Latvia)**
Название	**Используют ли органы государственной власти все возможности по эффективному управлению ИКТ-инфраструктурой? (Has Public Administration Used All Opportunities for Efficient Management of ICT Infrastructure?)**
Дата	**07/06/2019**
Ссылка	

ВОА Латвии провел аудит оптимизации управления цифровой инфраструктурой в органах государственной власти. Повышение эффективности государственного управления в целом невозможно без эффективного использования и оптимизации данной инфраструктуры. По мнению аудиторов, лишь одно ведомство – Министерство юстиции добилось серьезных успехов в централизации собственных цифровых систем и оптимизации их работы.

Аудиторы полагают, что для успеха цифровой трансформации госорганов необходимо выполнение ряда условий:

Наличие системы сбора и анализа максимально-полного объема данных;

Последовательный план внедрения цифровых инструментов и платформ в работу госоргана;

1. Система обратной связи и постоянной оценки эффективности внедрения цифровых решений.
2. Последовательный план внедрения цифровых инструментов и платформ в работу госоргана;
3. Система обратной связи и постоянной оценки эффективности внедрения цифровых решений.

ВОА	**Государственное контрольное управление США (Government Accountability Office of the United States, GAO U.S.)**
Название	**Информационные технологии: Агентствам необходимо разработать и внедрить планы модернизации критически-важных устаревших систем (Information Technology: Agencies Need to Develop and Implement Modernization Plans for Critical Legacy Systems)**
Дата	**27/04/2021**
Ссылка	

По оценкам Государственного контрольного управления (GAO U.S.) США ежегодно по состоянию на 2021 г. тратят до 100 млрд долл. на поддержание работы и обслуживание информационных систем. Вместе с тем, многие информационные системы, используемые органами государственной власти в США или, являются устаревшими, или стремительно устаревают. Стоимость поддержания и обслуживания данных систем неуклонно растет. Кроме того, данные системы становятся все более уязвимы для кибератак и других типов угроз их функционированию. ВОА США выделило ряд информационных систем, срок использования которых составляет от 8 до 51 года. Как правило модернизации и/или создания и внедрения новых систем сталкивается с проблемой переноса и адаптации данных и процессов их обработки и использования, а также в высокой степени интеграции устаревших систем как друг с другом, так и с процессами государственного управления. Наконец, немаловажным является проблема наличия специальных компетенций персонала по работе с устаревшими системами.

В рамках своих рекомендаций ВОА США выделяет необходимость разработки комплексных планов модернизации и/или замены данных информационных систем. При этом, эти планы должны соответствовать ряду критериев:

- учет ключевых потребностей заказчика в части повышения эффективности работы госоргана при внедрении новых систем;
- соответствие бюджетным ограничениям;
- срок внедрения новой системы и связанные с этим вопросы повышения компетенций сотрудников.

ВОА	**Государственное контрольное управление США (Government Accountability Office of the United States, GAO U.S.)**
Название	**Интернет вещей: Информация по использованию технологии федеральными ведомствами (Internet of Things: Information on Use by Federal Agencies)**
Дата	**13/08/2020**
Ссылка	

Интернет вещей (IoT) представляет собой совокупность информационных систем, собирающих/анализирующих данные, обменивающихся полученными данными между собой и при необходимости выполняющих определенные физические действия. В ходе своего исследования GAO проанализировал как даннае технология используется органами государственной власти в США. В исследовании систематизирована информация по ведомствам, использующим данную технологию, сферам применения IoT, возможностях и рисках применения технологии, а также по внутреннему регулированию использования IoT. Несмотря на привлекательность использования технологии, многие ведомствами отказываются внедрять IoT, как причине нехватки средств для долгосрочных инвестиций в обновление технической базы, так и по причине того, что их руководство не видит долгосрочные положительные эффекты от внедрения данной технологии.

ВОА	**Федеральное контрольно-ревизионное управление Швейцарии (Swiss Federal Audit Office)**
Название	**Возможности синергии информационных порталов федеральных органов государственной власти (Potential Synergies in Federal IT-Portals)**
Дата	**17/09/2021**
Ссылка	

Взаимодействие между органами государственной власти с одной стороны и бизнесом и гражданами с другой осуществляется либо с помощью ряда профильных сайтов, либо с помощью порталов и цифровых платформ, объединяющих несколько функций и услуг. Данные платформы разрабатывались, функционировали и совершенствовались независимо друг от друга.ВОА Швейцарии изучил возможности синергии работы нескольких федеральных информационных порталов. По мнению аудиторов, для устранения дублирующих функций, а также повышения эффективности работы платформ потребуется системная и долгосрочная работа.

ВОА полагает, что ключевым вопросом является координация стратегий развития федеральных информационных порталов и синхронизация обновления их функций, баз данных и т.д. Кроме того, важно добиться согласованного видения долгосрочной архитектуры государственных цифровых решений.

BOA	**Национальное контрольно-ревизионное управление Швеции (Swedish National Audit Office)**
Название	**Автоматизированное принятие решение в сфере государственного управления – эффективность и оперативность при недостатке контроля и исправления ошибок (Automated decision-making in public administration – effective and efficient, but inadequate control and follow-up)**
Дата	**18/12/2020**
Ссылка	

Национальное управление по аудиту Швеции (BOA Швеции) в 2020 г. провело аудит использования автоматизированных систем принятия решений в сфере государственного управления. BOA отмечает, что несмотря на то, что широкое внедрение подобных систем позволяет существенно повысить как эффективность, так и соответствие принимаемых решений действующему законодательству, вместе с тем данные системы часто страдают от ошибок операторов, а также заложенных и проявившихся в ходе их создания и настройки. Возможные ошибки подобных систем могут иметь серьезные последствия для граждан и подрывать доверие к государственной власти со стороны населения.

BOA Швеции предлагает уделить особое внимание разработке «баз знаний» и алгоритмов работы с автоматизированными системами принятия решений. Данные базы и алгоритмы должны содержать ответы на наиболее часто возникающие у операторов вопросы, а также стандартизированные решения для наиболее распространенных проблем.

ВОА	**Национальное контрольно-ревизионное управление Швеции (Swedish National Audit Office)**
Название	**Устаревшие ИТ-системы – препятствие на пути эффективной цифровизации (Obsolescent IT systems – an obstacle to effective digitalisation)**
Дата	**4/12/2019**
Ссылка	

В 2019 г. ВОА Швеции провел аудит цифровых систем, используемых 60 крупнейшими органами государственной власти. Аудиторы отмечают, что большинство госорганов продолжают использовать устаревшие системы. Помимо нехватки финансирования, к основным причинам сохранения данных систем в работе ВОА относит следующие:

1. Значительная часть госорганов не имеет четкой стратегии и принципов работы цифровыми системами;
2. Сотрудникам и руководству госорганов не хватает профильных навыков работы с цифровыми системами;
3. Отсутствует процесс постоянной оценки соответствия информационных систем потребностям и задачам госоргана;

Правительство не приняло соответствующих мер, направленных на исправление ситуации (в ч. создания единой цифровой экосистемы для госорганов, формирования централизованного запроса на оценку эффективности цифровых систем, содействие госорганам в обновлении информационных систем и регулярный контроль за данным процессом).

На основе полученных данных ВОА Швеции выделяет ряд рекомендаций для госорганов по работе с устаревшими системами:

1. Необходимо выделить ответственный орган/лицо в системе госуправления, которое будет осуществлять мониторинг работы устаревших систем и оказывать помощь ведомствам, столкнувшимся с данной проблемой;

2. Требуется разработка специальных инструментов оценки (методологии и метрик) эффективности использования ИТ-систем, а также потребностей в их модернизации и/или замене.

ВОА	**Национальное управление по аудиту Эстонии (National Audit Office of Estonia)**
Название	**Управление рисками в сфере развития программного обеспечения в публичном секторе (Management of software development projects in public sector)**
Дата	**10/09/2021**
Ссылка	

ВОА Эстонии проанализировал на примере развития девяти государственных информационных систем, могут ли государственные проекты развития программного обеспечения оказаться неудачными, а также какие проблемные места существуют в данной сфере. Аудит показал, что из девяти проектов по развитию программного обеспечения четыре оказались неудачными. В качестве причин неудачи проектов, аудиторы указывают следующие:

1. слабое или неадекватное планирование приводит к устареванию систем еще на стадии разработки;
2. отсутствие учета потребностей и квалификации пользователей;
3. постоянное и быстрое изменение регулирующих актов, норм и законодательства в данной сфере;
4. недостаточность знаний и навыков руководителей проектов и программ;
5. некомпетентность подрядчиков, отсутствие должного контроля на всех стадиях реализации проектов;
6. плохая согласованность действий заказчика и исполнителей.

По мнению ВОА, успех внедрения информационных систем зависит от ряда факторов:

1. Основные процессы в рамках госоргана должны быть определены и оптимизированы до внедрения информационных систем;
2. Внедрение систем должно осуществляться компетентными сотрудниками;
3. Госслужащие (пользователи) должны привлекаться к разработке технического задания системы на этапе проектирования;
4. Необходимо создать форму обратной связи с пользователями с оценкой эффективности системы;
5. Разработка систем должна учитываться в законодательном процессе.

ВОА	**Национальное управление по аудиту Эстонии (National Audit Office of Estonia)**
Название	**Управление информационными технологиями в государственном секторе (Overview of information technology expenditure and investments in Ministries and their authorities)**
Дата	**19/12/2019**
Ссылка	

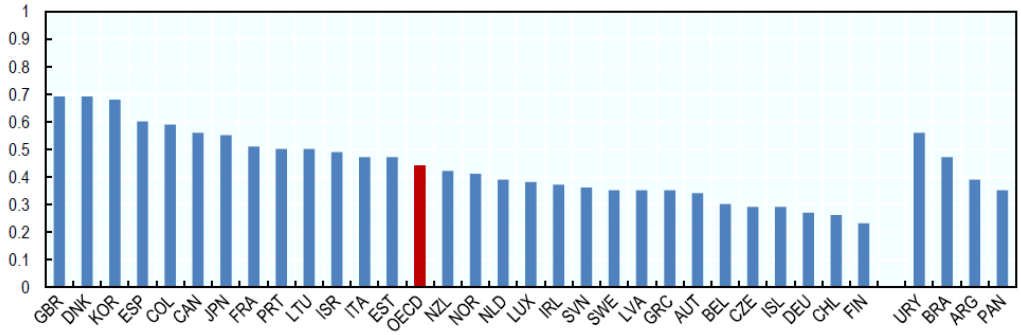
ВОА Эстонии провел исследование динамики роста расходов и инвестиций в государственную информационную инфраструктуру. Аудиторы ВОА отмечают, что темпы роста расходов на информационную инфраструктуру в органах государственной власти существенно опережают бюджетные ассигнования и инвестиции. Одной из ключевых статей расходов, вызывающих опасения ВОА, являются расходы на персонал. Однако рост зарплат не повлиял на снижение «текучки» кадров в сфере ИТ-систем органов государственной власти.

Аудиторы отмечают, что «текучка» кадров частично связана с неравномерностью роста доходов в государственном секторе и в целом в экономике. Так, в обозначенный период доходы ИТ-специалистов в госорганах увеличились на 6.7%, в то время как в среднем по стране рост доходов составил 7.4%.

Технологии анализа данных

В условиях стремительного развития государственных информационных систем возрастает объем уникальных данных. Усиливая информационно-аналитическую составляющую, технологии анализа данных (data analysis) и технологии «больших данных» (big data) повышают эффективность управленческих решений, особенно в таких областях, как здравоохранение, занятость населения, экономическое регулирование, борьба с преступностью и реагирование на чрезвычайные ситуации (data-driven decision management).

В своих программных документах государства повсеместно объявляют большие данные стратегическим активом, используя их для определения стратегических целей в сфере государственной политики, оценки позитивных и негативных последствий сформулированных решений, выявления ранее скрытых зависимостей между процессами, формирования систем риск-менеджмента и профилактики нарушений. Согласно индексу развития цифрового правительства Организации экономического сотрудничества и развития (ОЭСР), на международной арене лидерами в сфере госуправления, основанного на данных (data-driven public sector), выступают Великобритания, Дания и Республика Корея.



Note: Data are not available for Australia, Hungary, Mexico, Poland, Slovakia, Switzerland, Turkey and the United States.
Source: OECD Survey on Digital Government 1.0.

Источник: ОЭСР, Индекс развития цифрового правительства

В условиях возрастающего интереса госорганов к использованию больших данных возрастает важность проведения соответствующего аудита. В соответствии с отраслевыми исследованиями[1], аудит больших данных включает три взаимосвязанных уровня: технологический, управленческий и стратегический. Они соответственно ориентированы на оценку:

[1] Appelbaum D, Kogan A, Vasarhelyi M A. Big Data and Analytics in the Modern Audit Engagement: Research Needs. Auditing A Journal of Practice & Theory, 2017, 36(4):1-27; Al-Sai Z, Abdullah R, Husin H. Critical Success Factors for Big Data: A Systematic Literature Review. IEEE Access, 2020:1-1

- Эффективности внедрения **инновационных технологий** в работу госоргана. Ключевые параметры оценки – качество сбора данных, разнообразие методов их обработки, развитость и доступность инфраструктуры.
- Эффективности **функциональной структуры** организации в контексте использования больших данных. Особое внимание уделено оценке качества профессионального обучения, взаимодействия между подразделениями по вопросам использования больших данных, работы технологических центров по обработке больших данных.
- Соответствия между ожидаемыми и полученными **результатами** от внедрения технологий анализа больших данных. Критериями оценки служат: общее число выявленных неточностей при работе алгоритмов интеллектуального анализа данных (эффективность), социальный эффект от повышения прозрачности информации (легитимность), точность риск-менеджмента (прогнозирование).

Несмотря на неоспоримые преимущества технологий анализа больших данных, существуют определённые риски и ограничения их использования. Среди основных проблем – обеспечение необходимого качества данных, под которым принято понимать сумму следующих признаков:

- **полнота** (отсутствуют пробелы в данных, препятствующих их анализу или использованию);
- **комплексный характер** (все элементы, описывающие целевой объект/событие/ситуацию, включены в набор данных);
- **своевременность** (регулярные обновления);
- **понятность** (включают метаданные и машиночитаемый формат);
- **точность** (имеющиеся данные верны и четко отражают текущее состояние объекта, процесса и/или явления);
- **непротиворечивость** (имеющиеся ряды данных не противоречат друг другу, использование разных рядов не влияет на точность выводов);
- **уникальность** (элементы не повторяются в пределах одного набора данных);
- **проверяемость** (исходные данные и каталоги данных получены с открытых информационных систем правительства и/или внутри госаппарта);
- **машино-читаемость** (данные представлены в форматах, которые могут быть использованы машинными алгоритмами сразу и/или с минимальной обработкой человеком);
- **совместимость** (стандарты, семантика, общие идентификаторы данных доступны к обработке на наиболее распространенных технологических платформах);
- **защищенность** (соблюдены все требования по защите персональных и/или других конфиденциальных данных).

Эффективный мониторинг и контроль качества данных требует от госучреждений разработки четкой методологии управления данными, а также оценки их достоверности. Для достижения нужного качества данных, помимо их первичной обработки (data-cleaning), эксперты ОЭСР рекомендуют выполнять регулярные и случайные аудиты данных. Задачи таких контрольных мероприятий – оценка данных на соответствие общепринятым стандартам и заданным целям, нормам этики, включая обеспечение неприкосновенности частной жизни, и законодательства. Подобные меры призваны исключить подстраивание фактических данных под ожидания.

Руководство по проведению аудита с помощью анализа данных Рабочей группы ИНТОСАИ по работе с большими данными (WGBD) (Guidance on Conducting Audit Activities with Data Analytics) включает следующие методы верификации данных при проведении аудита:

- проверка **полноты данных** с помощью сравнения количества и объема частично структурированных и неструктурированных данных внутри массивов, предоставленных объектом аудита;
- проверка **ограничений целостности** реляционных моделей, включая ограничения первичного ключа (primary key constraints), ссылочные ограничения (referential constraints), пользовательские ограничения целостности (user-defined integrity constraints) и т. д.;
- проверка **соответствия данных** исходной информации (финансовой отчетности);
- проверка **общего количества** данных, статистических показателей основных переменных, а также подлинности значений в массивах данных путем расчета и агрегирования. Например, проверка соответствия диапазона основных переменных диапазону, представленному в отчете об операционной деятельности, путем расчета максимального и минимального значений основных переменных и агрегирования;
- проверка **корректности** заполнения отчетности (наличие прерывистых и повторяющихся значений, диапазон дат и т.д.).

Отдельный комплекс проблем в сфере больших данных связан с предоставлением открытого доступа к государственным данным для граждан. Политика по совершенствованию правого регулирования информационной политики стран ОЭСР нацелена на снижение административных барьеров и повышение доступности государственных данных. В 29 из 32 государств – членов ОЭСР центральные/федеральные правительства требуют, чтобы данные были доступны бесплатно, в машиночитаемых форматах и с соответствующими метаданными. Из 32 государств – членов ОЭСР 28 стран требуют, чтобы данные были доступны с открытой лицензией.

Кроме того, многие государства – члены ОЭСР взяли на себя обязательство публично продвигать принцип открытости государственного управления. Среди приоритетных направлений – увеличение числа программ повышения осведомленности о преимуществах открытых государственных данных и их повторного использования, повышение цифровой грамотности госслужащих.

В рамках Европейского союза (ЕС) Директива ЕС 2019/1024 от 20 июня 2019 г. играет центральную роль в поддержке государственных усилий по повышению открытости данных, содействуя внедрению инноваций и надлежащему управлению. Статья 16 прямо призывает государства «способствовать созданию данных на основе принципов открытости по замыслу и по умолчанию» (open by design and by default).

Несмотря на трудности с обеспечением открытых данных и исходного кода в госсекторе, данные меры способствуют прозрачности, подотчетности и общественному контролю граждан над решениями и результатами государственной политики. В этих условиях целесообразным представляется:

- **Продвигать создание качественных экосистем данных**, предоставляя населению неограниченный доступ к источникам данных и помогая обеспечить справедливое распределение информации в обществе.
- **Предоставлять открытый доступ к дезагрегированным данным** в соответствии с требованиями конфиденциальности, безопасности и соблюдения прав собственности. Анонимные и детализированные (granular)[2] открытые данные могут быть использованы для выявления актуальных социально-экономических проблем, принятия решений, основанных на фактах. В свою очередь, подобные наглядные результаты будут способствовать росту доверия к инструментам анализа данных как внутри госсектора, так и в обществе.
- **Сделать исходный код открытым для общественного контроля и аудита**, в особенности, в тех случаях, когда личные данные или наборы данных обрабатываются в рамках проектов цифрового правительства.

[2] Уровень детализации на основе имеющихся данных. Детализация включает данные на один уровень ниже предыдущего (в ч. – часы, минуты, секунды и т.д.). Максимальный уровень детализации подразумевает максимальный уровень подробности набора данных.

Кейсы

ВОА	**Управление по аудиту Австралии (Australian National Audit Office)**
Название	**Использование анализа данных для риск-ориентированного планирования аудита эффективности (Using data analytics for risk-based performance audit planning)**
Дата	**25/10/2021**
Ссылка	

В рамках опроса Счетной палаты Российской Федерации, посвященного развитию принципов Московской декларации ИНТОСАИ, Управление по аудиту Австралии подготовило обзор использования технологий анализа данных при проведении аудита предоставления грантов правительства. В основе анализа использован принцип сравнения баз данных проведенных тендеров и заключенных контрактов, наряду с основаниями заключения госконтрактов (был ли контракт заключен по итогам многоступенчатой стандартной процедуры оценки или вне ее). Это помогло выявить случаи, когда контракты заключались до официального закрытия тендера, что в свою очередь позволяет определить контракты с высоким риском нарушений.

Управление по аудиту Австралии полагает, что использование элементов анализа данных при проведении аудиторских мероприятий позволяет:

1. Определить наиболее рискованные проекты в рамках всех расходов правительства;
2. Выделить случаи, требующие более пристального изучения при проведении дальнейших аудиторских мероприятий;
3. Выявить условия, способствующие нарушениям при проведении тендеров;
4. Своевременно корректировать программу аудиторских мероприятий на уровне ВОА.

ВОА	**Национальное контрольно-ревизионное управление Великобритании (UK National Audit Office)**
Название	**Вызовы использования данных в работе правительства (Challenges in using data across government)**
Дата	**21/06/2019**
Ссылка	

Правительство Великобритании активно использует данные для улучшения как политики в разных сферах, так и для повышения качества государственного управления и предоставления лучших услуг гражданам страны. Вместе с тем, существует ряд серьезных вызовов, связанных прежде всего с вопросами безопасного использования и хранения данных (в т.ч. и персональных данных граждан), а также с поиском баланса интересов стейкхолдеров, связанных с работой с данными, в целях обеспечения устойчивого и эффективного инвестирования государственных средств в работу с данными.

ВОА Великобритании полагает, что для дальнейшего развития использования данных на уровне правительства требуется формирование согласованной стратегии по сбору, сортировке, хранению и использованию персональных данных граждан госорганами. Особую роль в этом вопросе играет максимально-широкий охват ведомств, чтобы исключить дублирование функций, полномочий, а также запросов.

ВОА	**Национальное контрольно-ревизионное управление Великобритании (UK National Audit Office)**
Название	**Руководство по управлению данными в госсекторе (Improving government data: A guide for senior leaders)**
Дата	**21/07/2022**
Ссылка	

ВОА Великобритании разработал руководство по управлению данными в госсекторе. ВОА отметил, что данные – это один из наиболее значимых активов правительства и крайне важно совершенствовать обмен, повышать качество, развивать соответствующие стандарты, формировать межведомственные наборы данных. В рамках руководства рассмотрено управление данными, которые собираются с целью эффективного предоставления государственных услуг. При этом ВОА подчеркивает, что документ может быть полезен также для управления данными, предназначенными для выработки политических решений. Документ призван способствовать деятельности руководства государственных органов: бухгалтеров, директоров, а также лиц, ответственных за предоставление государственных услуг.

BOA	**Управление Генерального аудитора Дании (Auditor General Office of Denmark)**
Название	**Отчет об открытых данных (Report on open data)**
Дата	**15/03/2019**
Ссылка	

Обеспечение доступа к данным правительства является одним из ключевых показателей открытости государства, а также помогает обеспечить экономический рост и развитие. В 2019 г. BOA Дании исследовал размещение открытых данных правительства страны в сети Интернет. По мнению аудиторов, отсутствие системности в размещении массивов данных (данные разбросаны по 88 источникам), а также проблема с определением органа, ответственного за размещение данных правительства, препятствуют открытости деятельности органов государственной власти.

BOA Дании выделяет ряд рекомендаций по дальнейшей работе с открытыми данными:

1. Сферы ответственности за работу по размещению открытых данных должна быть четко определены и разграничены между ведомствами;
2. При выборе данных для размещения в открытом доступе необходимо соблюдать принцип «открытости по умолчанию», т.е. все ведомства обязаны размещать данные в открытом доступе, в случае, если нет веских причин не делать этого;
3. Требуется расширение и регулярное обновление каталога открытых данных.

BOA	**Управление Генерального аудитора Дании (Auditor General Office of Denmark)**
Название	**Курс «Положения Московской декларации ИНТОСАИ: опыт BOA»**
Дата	**15/09/2021**
Ссылка	

В рамках курса «Положения Московской декларации ИНТОСАИ: опыт BOA»[3], BOA Дании в 2021 г. подготовил выступление на тему «Аналитика данных в аудите». В качестве примера работы с использованием цифровых источников была приведена проверка датской налоговой службы. BOA использовал программное обеспечение для статистического анализа STATA при работе с большим набором данных. Этот подход позволил лучше понять объем долга датского правительства, основных должников и методы эффективного управления долгом.

[3] Курс представлен на цифровой платформе Цифрового университета для сообщества ИНТОСАИ, www.u-intosai.org

BOA	**Национальное контрольно-ревизионное управление КНР (National Audit Office of China)**
Название	**Аудит с использованием технологий анализа данных в эпоху больших данных (Audit Data Analysis in the Big Data Era)**
Дата	**15/09/2021**
Ссылка	

BOA КНР систематизировал опыт использования технологий анализа данных и работы с большими данными при проведении проверок. Аудиторы подтверждают, что использование разнообразных инструментов анализа данных для формирования аудиторских заключений стало распространённой практикой не только внутри самого BOA, но и внутри региональных контрольных управлений. Кроме того, подтверждается, что органы государственной власти активно привлекают технологии и специалистов в сфере анализа данных и работы с большими данными при выработке государственных программ и проектов. Вместе с тем, в работе с данными зачастую используются наиболее простые и базовые инструменты (такие как, например, Excel), в то время как использование языков программирования и специализированных решений остается редкой практикой. Кроме того, работа с данными осложняется отсутствием единого реестра данных и возможности оперативного обмена информацией, в т.ч. закрытого характера.

Технологии искусственного интеллекта (ИИ)

Интенсивное развитие и распространение цифровых технологий в последние десятилетия значительно меняют облик ключевых сфер общественной жизни. Среди приоритетных направлений технологического развития – искусственный интеллект (ИИ), робототехника, блокчейн, технологии виртуальной и дополненной реальности.

Пандемия COVID-19 стала драйвером развития технологии ИИ. В условиях перегрузки национальных систем здравоохранения и жестких эпидемиологических ограничений ИИ активно применялся и продолжает применяться для диагностики заболеваний, прогнозирования течения болезни и дальнейшего распространения вируса. По оценкам Центра по изучению искусственного интеллекта Стэнфордского университета (Stanford Institute for Human-Centered Artificial Intelligence), частные инвестиции в ИИ в 2021 г. в два раза превысили показатели 2020 г. и составили 93,5 млрд долл. США. Международная корпорация данных (International Data Corporation, IDC), в свою очередь, прогнозирует рост глобальных расходов на развитие систем искусственного интеллекта до 204 млрд долл. в США к 2025 г.

Повсеместное внедрение технологий ИИ приведет к росту мирового ВВП на 14 % (15,7 трлн долл. США) в 2030 г., говорится в докладе PricewaterhouseCoopers (PwC) «Макроэкономическое влияние искусственного интеллекта» (The macroeconomic impact of artificial intelligence). Эксперты компании МакКинзи (McKinsey) ожидают, что к 2030 г. около 70 % компаний будут использовать, как минимум, один из типов технологии ИИ, что принесет мировой экономике 13 трлн долл. США и обеспечит рост мирового ВВП на 1,2% в год.

При положительной динамике государственных инвестиций в информационные технологии все больше вложений приходится именно на искусственный интеллект. В 2021 г. федеральное финансирование научных исследований в области ИИ в США выросло на 50% по сравнению с 2020 г. и достигло 6 млрд долл. США[4]. Технологии ИИ предоставляют уникальные возможности для повышения эффективности государственного управления, снижая издержки и обеспечивая высокую точность прогнозирования управленческих решений. Исследование Делойт (Deloitte) показывает, что автоматизация рабочих процессов с использованием ИИ сэкономит до 30% рабочего времени государственных служащих.

[4] В 2021 г. в России стартовал Федеральный проект «Искусственный интеллект», в рамках которого в ИИ будет вложено 24,6 млрд рублей в течении 5 лет. Из запланированных 4,7 млрд рублей в 2021 г. исполнено 99% утвержденного бюджета.

Согласно данным[5] ОЭСР, более 60 стран разработали стратегии по развитию искусственного интеллекта. Национальные «дорожные карты» различаются по целям, срокам и механизмам реализации, отраслевой направленности, бюджетам и характеру государственного участия. Из 230 проектов в области ИИ, инициированных государственными учреждениями стран – членов Европейского союза (ЕС), 7 реализуется в сфере образования, 4 – культуры, 41 – здравоохранения, 14 – ЖКХ, 3 – защиты окружающей среды, 40 – экономики, 27 – обеспечения общественного правопорядка, 4 – обороны, 16 – социальных услуг, 76 – государственных услуг.

Проекты в области ИИ в ЕС

Характер государственного участия в проектах в сфере ИИ различается. Эксперты ОЭСР выделяют следующие варианты:

- **Инвестор**. Государство финансирует разработку и содействует внедрению новых технологий.
- **Заказчик**. Государство осуществляет закупки цифровых продуктов или участвует в разработке новых программных решений через механизм государственно-частного партнерства (ГЧП).

[5] По состоянию на апрель 2020 г.

- **Регулятор**. Государство, следуя научно-техническому прогрессу, своевременно обновляет соответствующую нормативно-правовую базу.
- **Стандартизатор**. Государство организует разработку национальных стандартов с привлечением всех заинтересованных сторон, проводит оценку их соответствия современному уровню технического развития.
- **Владелец данных**. Государственные органы хранят и обрабатывают огромные массивы данных, обеспечивают их безопасность и целостность.
- **Поставщик услуг**. Государственные цифровые платформы взаимодействуют с гражданами, активно используя технологии ИИ.

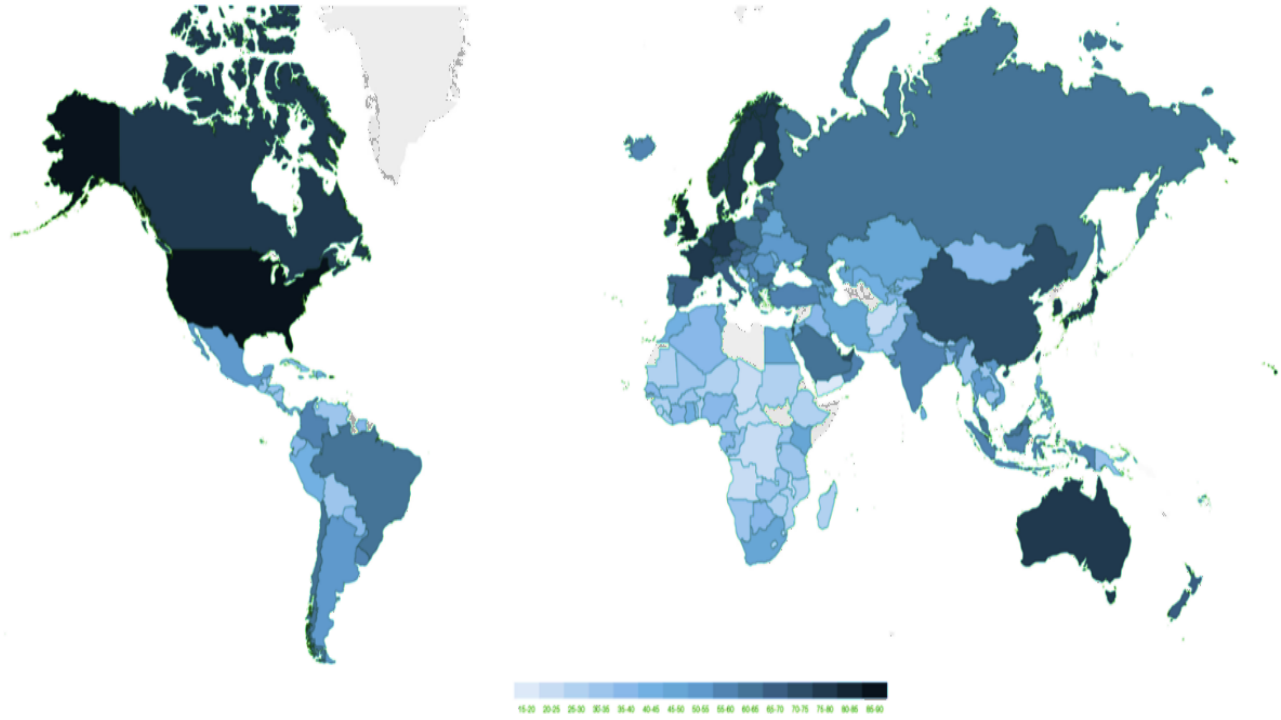
Авторы доклада ОЭСР «Привет, мир: искусственный интеллект и его использование в государственном секторе» (Hello, World: Artificial intelligence and its use in the public sector) выделяют следующие факторы развития ИИ:

- **Развитие научного потенциала**. За последние десятилетия накоплен обширный и разнообразный объем знаний в области ИИ, усовершенствованы компьютерные алгоритмы и языки программирования.
- **Технический прогресс**. Увеличение вычислительной мощности обеспечивает более высокую производительность компьютеров и скорость обработки данных. Затраты на хранение данных также резко снизились: с 1 млн долл. США за 1 гигабайт в 1967 г. до 2 центов США в 2017 г.
- **Доступность технологий**. Бесплатные сервисы для совместной работы и управления проектами, онлайн-курсы и учебные пособия способствуют повышению цифровой грамотности населения и более широкому использованию ИИ.
- **Увеличение объема данных**. Большие данные – главная движущая сила ИИ. Более 90% мировых цифровых данных создано в течение последних нескольких лет, и темпы их производства продолжают расти.

Несмотря на возросшее внимание к потенциалу ИИ, результаты оценки[6] готовности государств к внедрению ИИ-решений 2021 г. (Government AI Readiness Index 2021) свидетельствуют о существенной разнице в региональном технологическом развитии. Средний балл стран тропической

[6] В основе методологии – 42 индикатора, сгруппированных по трем направлениям: качество государственного управления (наличие целенаправленной стратегии развития ИИ и соответствующего правового регулирования), технологический потенциал (результаты инновационной деятельности, финансирование НИОКР, качество человеческого капитала), цифровая инфраструктура (доступность и репрезентативность данных).

Африки и Центральной Азии составляет 36,27, стран Северной Америки и Западной Европы – 76,75. Лидерами[7] отрасли являются США, Сингапур и Великобритания. Наличие высококвалифицированной рабочей силы, передовой исследовательской и технологической инфраструктуры, государственных мер поддержки инноваций также обеспечили высокие позиции стран Восточной Азии (5 стран региона входят в 20 лучших).



Источник: Доклад Oxford Insights «Индекс готовности правительств к внедрению ИИ» (Government AI Readiness Index 2021)

Эксперты Всемирного банка (ВБ) отмечают несколько перспективных сфер применения технологий ИИ в системе госуправления:

- **обработка** обращений граждан;
- **контроль** соблюдения законодательства и оценка рисков;
- финансовый **контроль** бюджетных расходов;
- **оптимизация** внутрикорпоративных операционных процессов;
- персонализированное **предоставление услуг** на основе анализа цифрового профиля гражданина;
- эффективное **распределение ресурсов** и помощь в принятии решений.

При всех потенциальных преимуществах ИИ существуют значительные риски: предвзятость искусственного интеллекта[8], информационная безопасность[9] и

[7] Россия занимает 38 место в рейтинге.
[8] Предвзятость по отношению к одной или нескольким группам людей возникает в результате обработки неполных, неточных, искаженных данных или ошибки/субъективности разработчиков. Системы ИИ необходимо постоянно совершенствовать по мере появления новых массивов данных и инструментов их обработки.
[9] Многие системы ИИ работают автономно, взаимодействуя друг с другом. В 2010 г. фондовые биржи в США упали на 10% из-за сбоя в алгоритмах, регулирующих торговые операции.

защита персональных данных. Среди ключевых рекомендаций по их минимизации – упреждающий контроль и мониторинг функционирования систем ИИ, совершенствование правого регулирования работы с данными, предоставление открытого доступа к эффективным цифровым моделям, использование нескольких систем ИИ для выполнения одной задачи, расширение международного сотрудничества.

16 ноября 2021 г. участники Генеральной конференции ЮНЕСКО (UNESCO General Conference) утвердили Рекомендации об этических аспектах искусственного интеллекта (Recommendation on the ethics of artificial intelligence) – первый международный документ по вопросам этического регулирования использования ИИ. Базовые этические принципы включают: уважение и защиту прав человека, защиту окружающей среды, обеспечение инклюзивности, неприкосновенность частной жизни, подконтрольность человеку, прозрачность. Документ призван стать правовой основой регулирования использования технологий искусственного интеллекта на глобальном уровне.

Тематические кейсы

Работа с обращениями граждан

С 14 октября 2020 г. посетителям **латвийского портала государственных услуг** «latvija.lv» помогает «виртуальный помощник» Эрик. В основе алгоритмов цифрового ассистента – история ответов на наиболее часто задаваемые вопросы граждан.

Здравоохранение

- В 2020 г. в Хорватии был разработан **«виртуальный доктор»**, который может обрабатывать 50 тыс. запросов ежедневно.
- InferRead™ CT Lung – программное обеспечение на основе ИИ, разработанное при поддержке **Европейского союза**, для анализа результатов компьютерной томографии и ранней диагностики коронавирусной инфекции.

Противодействие коррупции

- При поддержке **Всемирного банка** в Бразилии в 12 федеральных штатах запущена «умная» система оценки государственных закупок. ИИ анализирует 27 датасетов (250 млн точек данных), включая 15 млн электронных счетов на сумму более 100 млрд долл. США, сведения о 750 тыс. фирм, 30 тыс. новостных лент. За время работы система выявила 500 фирм, принадлежащих государственным служащим; более 420 фирм, выигравших тендеры у подставных компаний.
- **Академия наук Китая** совместно с органами внутреннего контроля Коммунистической партии разработали программное решение Zero Trust для оценки сведений о доходах, расходах и обязательствах имущественного характера госслужащих. Известно, что Zero Trust выявил нарушения в декларациях 8 721 государственного служащего.

Транспорт

- В 2017 г. **Департамент транспорта Лондона** запустил приложение на основе ИИ, которое предоставляет оперативную информацию об автобусных маршрутах, ближайших автобусных остановках, времени прибытия, загруженности метро.
- **Транспортная система г. Ханчжоу** регулируется с использование ИИ и технологии анализа больших данных. Система управления дорожным движением распознает дорожно-транспортные происшествия, замедление трафика и отправляет диспетчерские команды соответствующим службам.

Кейсы ВОА

ВОА	**Управление Генерального аудитора Норвегии (Office of the Auditor General of Norway)**
Название	**Аудит алгоритмов машинного обучения: Экспертный доклад для государственных аудиторов (Auditing machine learning algorithms: A white paper for public auditors)**
Дата	**14/10/2020**
Ссылка	

Активное внедрение технологий искусственного интеллекта (ИИ) и машинного обучения в органах государственного управления требует новых подходов к проведению внешнего государственного аудита. ВОА Бразилии, Великобритании, Германии, Нидерландов, Норвегии и Финляндии подготовили экспертный доклад с обзором ключевых рисков использования технологий ИИ и машинного обучения в госуправлении и предложениями по проведению аудита в рамках деятельности ВОА. Имеющиеся риски сгруппированы в 4 основных кластера:

1. Оптимизация алгоритмов ИИ и машинного обучения зачастую не учитывает требования соответствия законодательству, прозрачности и подотчетности госуправления;
2. Проблемы взаимодействия заказчика с подрядчиком, в результате чего техническое решение, основанное на технологиях машинного обучения, приводит к усложнению процессов госуправления;
3. Недостаток компетенций по использованию и развитию продуктов и решений, основанных на технологиях машинного обучения, внутри организации;
4. Проблема регулирования использования личных данных при обучении моделей и нейросетей (отсутствуют соответствующие руководства, выпущенные профильными ведомствами, ответственными за соблюдение безопасности личных данных).

ВОА	**Государственное контрольное управление США (Government Accountability Office of the United States, GAO U.S.)**
Название	**Искусственный интеллект: основы отчетности по использованию технологии федеральными ведомствами и другими организациями (Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities)**
Дата	**30/06/2021**
Ссылка	

С целью повышения подотчетности и ответственности в рамках использования систем искусственного интеллекта (ИИ) в рамках государственных программ, а также функционирования органов государственной власти, ВОА США в 2021 г. разработало руководство по системе отчетности в рамках использования ИИ. Руководство основано на 4-х взаимодополняющих принципах, среди которых управление (использование, контроль и отчетность в рамках внедрения ИИ в системы госуправления), работа с данными (использование качественных данных, полученных из надежных источников, а также их правильную обработку и анализ), оперативный контроль (обеспечение надежности и востребованности систем ИИ) и результативность (результат использования ИИ-систем должен соответствовать целям и задачам государственных программ и проектов).

ВОА	**Государственное контрольное управление США (Government Accountability Office of the United States, GAO U.S.)**
Название	**Оценка технологии: Искусственный интеллект: новые возможности, вызовы и последствия применения (Technology Assessment: Artificial Intelligence: Emerging Opportunities, Challenges, and Implications)**
Дата	**28/03/2018**
Ссылка	

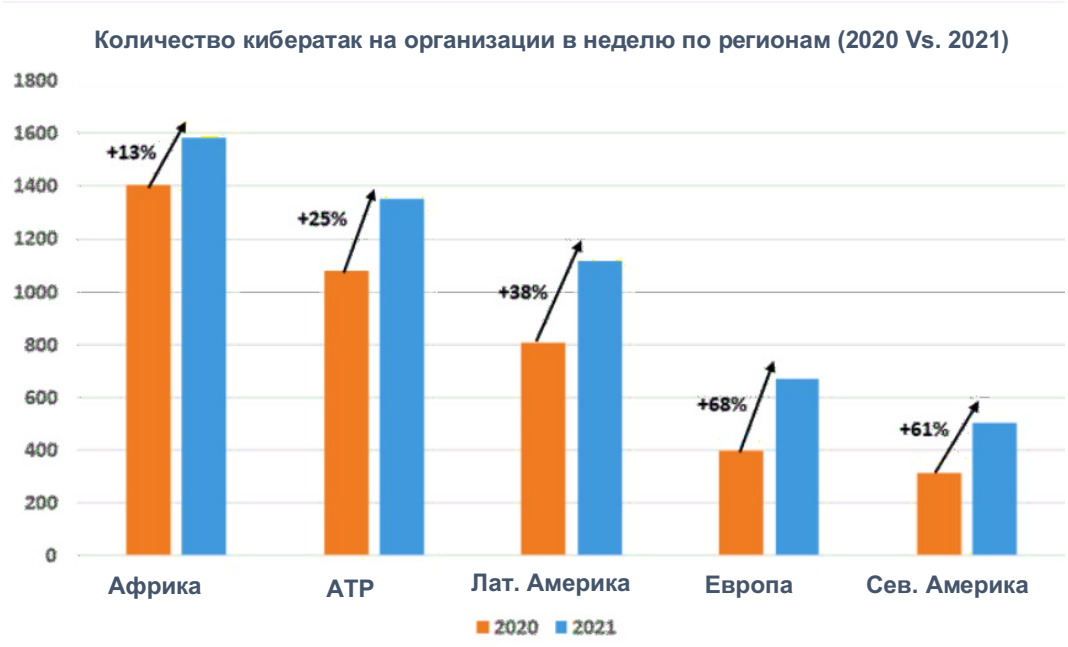
Для оценки последствия, а также вызовов, к которым может привести широкое внедрение технологий искусственного интеллекта (ИИ) ВОА США провел экспертное мероприятие в формате форума. Среди ключевых сфер, на которые обратили внимание участники – вопросы кибербезопасности, автономных автомобилей, правосудия и финансовых услуг. Эксперты отмечают, что, хотя преимущества развития ИИ в большинстве сфер очевидны, активное внедрение технологии в повседневную жизнь сталкивается с рядом серьезных вызовов. Среди основных вызовов – недостаточность данных для обучения нейросетей, нехватка компетенций сотрудников, этические риски.

Кибербезопасность

Цифровая трансформация способствует повышению качества и эффективности государственного управления, оптимизации финансовых и кадровых ресурсов.
В условиях растущей цифровой взаимозависимости, ускоренной пандемией COVID-19, и усложнения ландшафта угроз[10] возрастает необходимость обеспечения безопасности технологической инфраструктуры государственных институтов и защиты персональных данных граждан.

По оценкам Всемирного экономического форума (ВЭФ), в 2020 г. общее количество выявленных вредоносных программ увеличилось на 358%, программ-вымогателей – на 435%. Как отмечают эксперты организации, 95% проблем в сфере кибербезопасности связаны с человеческим фактором. При этом мировой дефицит специалистов в области кибербезопасности составляет 3,5 млн человек.

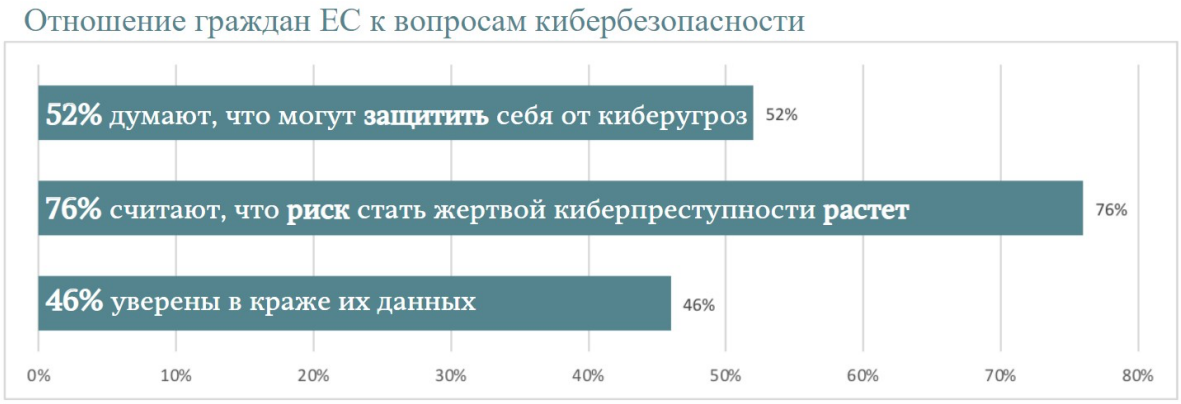
Согласно результатам анализа Check Point Research[11], в 2021 г. количество кибератак на корпоративные сети в неделю выросло на 50% (по сравнению с 2020 г.). Средний международный показатель составил 925 кибератак в неделю на организацию. Самый значительный рост количества кибератак зафиксирован в Европейском регионе.



Источник: Доклад Check Point Research

[10] Ландшафт угроз (threat landscape) — совокупность выявленных и потенциальных киберугроз для определенной отрасли, группы пользователей, конкретного периода времени.
[11] Подразделение компании Check Point Software Technologies Ltd – международной компании, работающей в сфере IT-безопасности.

В соответствии с данными[12] Европейского агентства по кибербезопасности (European Union Agency for Cybersecurity, ENISA) основными объектами кибератак в 2021 г. стали: государственные административные учреждения (198 инцидентов), провайдеры цифровых услуг (152 инцидента), медицинские учреждения (143 инцидента), финансовый и банковский сектор (97 инцидентов), транспортный сектор (54 инцидента). Среди наиболее распространенных видов кибератак – программы-вымогатели (ransomware), криптоджекинг (cryptojacking)[13], утечки данных (data breaches), вредоносное ПО (malware), дезинформация (disinformation), пользовательские ошибки (non-malicious threats), угрозы доступности и целостности информации (threats against availability and integrity), атаки на поставщиков цифровых услуг (supply-chain attacks).



Источник: Опрос Special Eurobarometer 499, январь 2020 г.

Динамика появления новых цифровых угроз превышает возможности организаций по их предотвращению, об этом говорится в исследовании IBM «Финансовые последствия утечки данных в 2021 г.»[14] (Cost of a Data Breach Report 2021). Переход на удалённый режим работы в условиях пандемии COVID-19 был осуществлен в ущерб интересам информационной безопасности организаций. В 2021 г. средний финансовый ущерб от утечки данных составил 4,2 млн долл. США (за один инцидент) – рекордный показатель за последние 17 лет.

Подходы к оценке эффективности политики в области кибербезопасности, как и сама исследовательская область, находятся в стадии становления. На данный момент не существует общепринятого определения понятия «кибербезопасность» (cybersecurity). В рамках системы ООН используется определение Международного союза электросвязи (МСЭ). Эксперты организации рассматривают кибербезопасность как совокупность средств и

[12] Результаты за период с апреля 2020 г. по июль 2021 г.
[13] Криптоджекинг – несанкционированное использование устройств для генерации криптовалюты.
[14] В основе исследования – анализ данных утечек более 500 компаний в период с мая 2020 г. по март 2021 г. Всего организация проанализировала около 100 тысяч нарушений.

технологий, стратегий и руководящих принципов, которые могут быть использованы для защиты информационных, технических, кадровых ресурсов организации в цифровой среде. Другие международные организации[15] используют термин «информационная безопасность» (information security) как безопасность информации во всех ее формах и на любых носителях. В фокусе внимания Организации экономического сотрудничества и развития (ОЭСР) – оценка цифровой безопасности (digital security): анализ экономических и социальных последствий киберугроз.

Концептуальные подходы государств и международных организаций могут различаться, однако главной целью политики в сфере кибербезопасности остается обеспечение конфиденциальности, целостности и доступности информации («триада информационной безопасности[16]»).

Правовые меры	**В 167 странах действует законодательство в области кибербезопасности**
	В 133 странах существуют законы о защите персональных данных
	В 97 странах разработаны правовые механизмы защиты критической инфраструктуры
Технические меры	**В 131 стране функционируют Национальные центры информационной безопасности**
	В 101 стране действуют механизмы защиты детей от распространения незаконной информации в Интернете
Организационные меры	**В 127 станах разработаны национальные стратегии в области кибербезопасности**
	В 98 странах актуализированы национальные стратегии в области кибербезопасности
	60% из вышеуказанных 98 стран проводят оценку эффективности реализации стратегий в области кибербезопасности
Развитие профессионального потенциала	**В 142 странах провели информационные кампании по вопросам кибербезопасности**
	В 94 странах запущены научно-исследовательские программы в области кибербезопасности
Международное сотрудничество	**90 стран имеют двусторонние соглашения в области кибербезопасности**
	112 стран участвуют в многосторонних инициативах в области кибербезопасности
	В 2020–2021 гг. 140 стран приняли участие в международных мероприятиях, таких как конференции по кибербезопасности, образовательные семинары.

Источник: Доклад МСЭ «Глобальный индекс кибербезопасности» (Global Cybersecurity Index)

МСЭ отмечает повышение уровня кибербезопасности государств во всем мире. Согласно показателям Глобального индекса кибербезопасности[17]

[15] Международный стандарт ISO/IEC 27001:2013

[16] Перечень ключевых принципов информационной безопасности постоянно обновляется. В 2002 г. ОЭСР опубликовала модель информационной безопасности, состоящую из девяти принципов. Международный стандарт ISO/IEC 27001:2013 содержит 10 основополагающих принципов.

[17] Глобальный индекс кибербезопасности (Global Cybersecurity Index, GCI) впервые опубликован Международным союзом электросвязи (МСЭ) в 2015 г. и обновляется раз в два года. Задача проекта – оценка системы информационной безопасности 193 государств – членов МСЭ по 5 ключевым направлениям: правовые меры, технические меры, организационные меры, развитие профессионального потенциала и международное сотрудничество.

(Global Cybersecurity Index, GCI), к концу 2020 г. 127 стран утвердили национальные стратегии информационной безопасности, 142 – провели информационные кампании по вопросам кибербезопасности. Лидеры рейтинга – США (100 баллов), Эстония (99,48), Великобритания и Саудовская Аравия (по 99,54 балла); Южная Корея, Сингапур и Испания (98,52 балла); Россия, ОАЭ и Малайзия (98,06 балла).

Несмотря на достигнутый прогресс, остаются области, требующие дальнейшего улучшения – модернизация средств защиты критической инфраструктуры в соответствии с новыми киберугрозами, усиление правового регулирования работы с персональными данными, повышение общего уровня цифровой грамотности.

Среди ключевых рекомендаций МСЭ по повышению уровня цифровой безопасности государств: регулярный мониторинг эффективности реализации стратегии в области кибербезопасности, улучшение ресурсной базы национальных центров информационной безопасности, необходимость активизации международного сотрудничества и обмена лучшими практиками противодействия цифровым угрозам.

Кейсы

ВОА	**Счетный суд Австрийской Республики (Austrian Court of Audit)**
Название	**Координация усилий в сфере кибербезопасности (Coordination of Cyber-Security)**
Дата	**22/04/2022**
Ссылка	

В 2021 г. ВОА провел аудит эффективности систем кибербезопасности в ряде федеральных ведомств Австрии (Федеральная канцелярия, Министерство внутренних дел, Министерство обороны и Министерство иностранных дел). В фокусе внимания ВОА была оценка нормативной базы, стратегического и операционного управления в области кибербезопасности. ВОА выявил ряд недостатков, в частности, отсутствие планов по операционному управлению инцидентами в области кибербезопасности и недостаточно эффективная система управления рисками. ВОА подчеркнул необходимость улучшения стратегии ведомств в области информационной безопасности и рекомендовал создать постоянную группу реагирования на вызовы в киберпространстве, а также центр реагирования на чрезвычайные ситуации.

BOA	**Национальное контрольно-ревизионное управление Великобритании (UK National Audit Office)**
Название	**Руководство для аудиторских комитетов в сфере кибербезопасности и оценке рисков информационных систем (Cyber and information security: Good practice guide)**
Дата	**28/10/2021**
Ссылка	

BOA Великобритании подготовил Руководство для аудиторских комитетов в сфере проверки услуг в области кибербезопаности и оценки рисков использования информационных систем на основе актуальных требований правительства. В качестве ключевых вопросов, на которые требуется обратить внимание при аудите подобных систем и услуг указываются:

1. общий подход организации к вопросам кибербезопасности и управления рисками;
2. ресурсы, необходимые для обеспечения кибербезопасности;
3. отдельные вопросы, в частности - управления рисками в сфере информационной безопасности и данных, безопасность сетей, управление нештатными ситуациями, защита от вредоносного ПО, удаленная работа сотрудников и т.д.;
4. смежные области, в частности – облачные сервисы, исследования и разработка новых технологий.

ВОА	**Управление Генерального аудитора Дании (Auditor General Office of Denmark)**
Название	**Отчет о соответствии государственных ведомств двадцати минимальным техническим требованиям в сфере информационной безопасности (Five government authorities' compliance with 20 technical minimum information security requirements)**
Дата	**15/01/2022**
Ссылка	

По итогам результате аудиторской проверки, проведенной Управлением генерального аудитора Дании в 2021 г., аудиторы пришли к выводу, что Министерство финансов, Министерство юстиции, Министерство здравоохранения, Министерство климата, энергетики и ЖКХ и Министерство продовольствия, сельского и рыбного хозяйства не обеспечили соблюдение 20-ти технических минимальных требований к информационной безопасности, которые должны были быть выполнены к 1 января 2020 г.

ВОА	**Европейская счетная палата (European Court of Audits)**
Название	**Вопросы кибербезопасности в институтах, органах и агентствах ЕС: общий уровень готовности не соответствует угрозам (Special report: Cybersecurity of EU institutions, bodies and agencies: Level of preparedness overall not commensurate with the threats)**
Дата	**29/03/2022**
Ссылка	

В связи с многочисленными случаями хакерских атак на информационные системы Европейского союза, Европейская счетная палата провела аудит эффективности политики информационной безопасности институтов ЕС в период с января 2018 г. по октябрь 2021 г. Особое внимание в рамках аудита было уделено деятельности Агентства ЕС по кибербезопасности (European Union Agency for Cybersecurity, ENISA) и Группы реагирования на инциденты информационной безопасности ЕС (Computer Emergency Response Team, CERT-EU). По оценкам Европейской счетной палаты, уровень устойчивости информационных систем ЕС различается в зависимости от ведомства и в целом не соответствует текущим масштабам киберугроз. В частности, только 58% ведомств ЕС имеют согласованную на уровне своего руководства стратегию в области информационной безопасности. В качестве причин неподготовленности институтов ЕС к киберугрозам указаны: отсутствие системы оценки устойчивости информационных систем или ее непоследовательность;

- устаревшие корпоративные практики в области кибербезопасности;
- отсутствие системного обучения сотрудников по вопросам информационной безопасности, а также программ повышения квалификации для специалистов профильных подразделений;
- недостаточно разработанная система управления информационной безопасностью ведомств и выборочная оценка рисков;
- неравномерность финансирования программ по повышению уровня кибербезопасности в институтах ЕС;
- отсутствие внешнего аудита систем информационной безопасности у ряда ведомств.

Европейская счетная палата призвала институты ЕС более слаженно координировать работу информационных систем и последовательно подходить к разработке стратегий в области кибербезопасности. Европейской комиссии рекомендовано ввести обязательные правила кибербезопасности, увеличить финансирование Группы реагирования на инциденты информационной безопасности и способствовать межведомственному сотрудничеству по данному вопросу.

ВОА	**Контактный комитет высших органов аудита Евросоюза (Contact Committee of the Supreme Audit Institutions of the European Union)**
Название	**Компендиум по аудиту: Кибербезопасности в ЕС и странах-членах союза (Audit Compendium: Cybersecurity in the EU and its member states)**
Дата	**07/12/2020**
Ссылка	

7 декабря 2020 г. Контактный комитет высших органов аудита Евросоюза опубликовал Компендиум по аудиту систем кибербезопасности ЕС. Основанный на результатах исследований, проведенных высшими органами аудита стран – членов ЕС, сборник посвящен проблеме устойчивости критически важных информационных систем и цифровой инфраструктуры ЕС к информационным атакам. В нем представлена справочная информация о проблеме кибербезопасности, стратегических инициативах ЕС и нормативно-правовой базе; обозначены основные вызовы и риски, с которыми сталкиваются граждане и государства ЕС в результате ненадлежащего использования цифровых данных. В основу исследования легли результаты 12 проверок, проведенных контрольными ведомствами стран – членов ЕС и Европейской счетной палатой по вопросам, связанным с кибербезопасностью. Результаты проверок позволили выявить уязвимость цифровой инфраструктуры и систем хранения персональных данных (Эстония, Франция, Швеция), недостаточность ресурсного обеспечения и эффективности управления системой информационной безопасности (Ирландия, Латвия, Финляндия), несоответствия установленным европейскими регламентами стандартам безопасности (Польша, Португалия).

ВОА	**Государственное контрольное управление США (Government Accountability Office of the United States, GAO U.S.)**
Название	**Реакция федеральных органов государственной власти на инциденты с участием сетей SolarWinds и Microsoft Exchange (Federal Response to SolarWinds and Microsoft Exchange Incidents)**
Дата	**13/01/2022**
Ссылка	

ВОА США в 2022 г. проанализировал меры, которые федеральные агентства предприняли в ответ на хакерские атаки сетей SolarWinds и Microsoft Exchange. В январе 2019 г. сеть SolarWinds – компании из Техаса по разработке программного обеспечения, чьи услуги широко использует федеральное правительство США – подверглась взлому. В марте 2021 г. компания Microsoft сообщила об использовании уязвимостей для получения незаконного доступа к нескольким версиям Microsoft Exchange Server. Данные попытки взлома стали одними из наиболее масштабных хакерских атак, которые когда-либо проводились против федерального правительства и частного сектора США. ВОА отмечает, что по итогам хакерских атак федеральные агентства США пришли к нескольким выводам:

- координация с компаниями частного сектора способствовала повышению эффективности предпринятых мер по реагированию на инциденты;
- создание централизованной площадки для диалога между государственными учреждениями, а также компаниями из частного сектора улучшило координацию между всеми заинтересованными сторонами;
- обмен информацией между федеральными агентствами зачастую осуществлялся медленно и занимал длительное время;
- процесс сбора доказательств носил ограниченный характер из-за различий в практике хранения данных в разных ведомствах.

BOA

Государственное контрольно-ревизионное управление Финляндии (National Audit Office of Finland)

Название	**Отчет об исполнении рекомендаций по итогам аудита процесса организации кибер-безопасности (Supplement to the follow-up report: Organizing cyber protection)**
Дата	**12/04/2022**
Ссылка	

В 2022 г. BOA Финляндии провел оценку качества исполнения своих рекомендаций по повышению эффективности мер кибербезопасности, подготовленных по итогам аудита Министерства финансов в 2017 г. BOA пришел к выводу, что рекомендации были выполнены частично.

BOA отметил, что некоторые операционные процессы по внедрению мер кибербезопасности необходимо улучшить и предоставил объекту аудита рекомендации по повышению их эффективности:

- Министерству финансов рекомендовано учитывать вопросы кибербезопасности на всех этапах финансирования и «жизненного цикла» государственных проектов в сфере цифровизации;
- Также предложено установить постоянно действующий канал связи и обменом данными об угрозах и возможных противоправных действиях в цифровой среде между министерством и профильными ведомствами.

Компетенции и повышение потенциала сотрудников

Процесс цифровизации государственных органов должен происходить комплексно, и включать в себя не только внедрение новых информационных технологий, но и повышение цифровых компетенций сотрудников. По мнению экспертов Всемирного экономического форума (ВЭФ), одним из условий успешной цифровой трансформации является применение проектного управления. Компактные и горизонтальные организационные структуры расширяют возможности сотрудников, обеспечивая большую гибкость и скорость принятия решений. Распространенной практикой является создание внутри государственного органа отдельного подразделения, ответственного за внедрение инновационных подходов, а также представляющего собой центр компетенций для обучения и оказания поддержки в использовании новых технологий «на местах».

Помимо формирования проектных команд и масштабирования цифровых решений, важным остается повышение цифровых компетенций всех сотрудников государственных органов, а также обучение «гибким» навыкам (soft skills), необходимым для адаптации к изменениям среды. Традиционно сложившийся консервативный характер профессии государственного служащего может быть серьезной проблемой для внедрения прорывных технологий в этом секторе. По сравнению с трудностями освоения новых технологий, для руководителей и сотрудников государственных органов гораздо сложнее изменить устоявшиеся модели мышления, вследствие чего вопрос обучения и повышения квалификации остается острым и необходимым для повышения эффективности деятельности государства. В частности, выделяют ряд проблем, с которыми сталкиваются органы государственной власти при повышении цифровых навыков сотрудников:

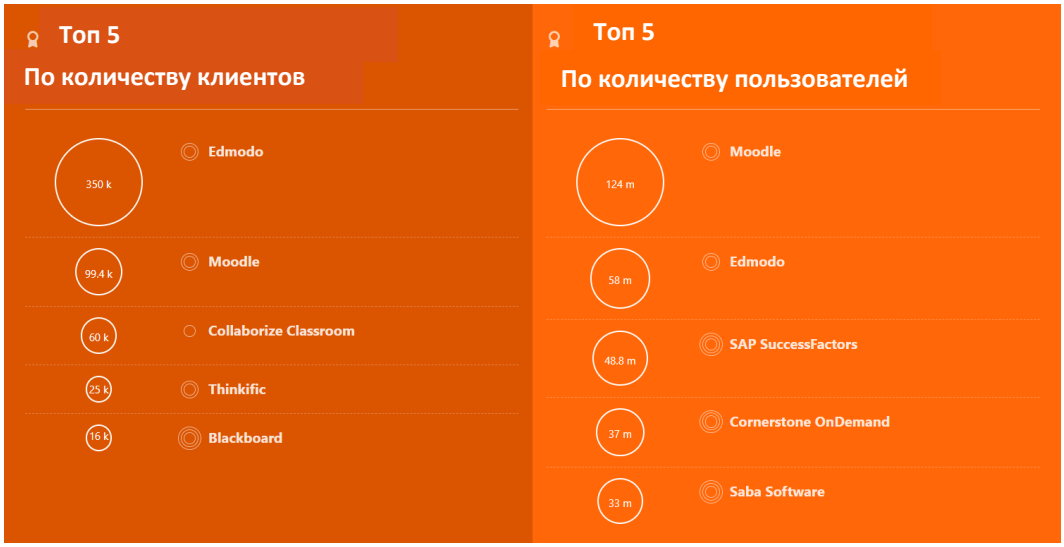
- Отсутствие четкого понимания целей, задач и рисков при организации обучения сотрудников (особо важным является избежать завышенных ожиданий, как в части скорости освоения, так и в вопросах применения новых навыков);
- Сложность вовлечения частных поставщиков образовательных услуг (необходимо создание гибких условий по контрактам, тщательное изучение рынка образовательных услуг);
- Учет необходимости работы с устаревшими системами и постоянный процесс обновления навыков;
- Подбор правильного сочетания необходимых навыков под конкретные задачи в сфере государственного управления;
- Правильный выбор способа подачи информации;
- Обеспечение финансирования и материального стимулирования сотрудников, обучающихся новым навыкам.

При этом важной проблемой является отсутствие понимания, каким именно набором компетенций должны обладать сотрудники для успешной цифровой трансформации в каждом конкретном государственном органе.

Не менее актуальными в процессе обучения сотрудников являются обмен передовыми практиками, опытом и знаниями между государственными органами различных стран. Этому способствует проведение международных конференций, заседаний рабочих групп, вебинаров и пр., а также создание платформ для обмена опытом. Только за 2021 г. по инициативе Международной организации высших органов аудита (ИНТОСАИ) и ее членов было проведено свыше 70 мероприятий, посвященных вопросам цифровизации как высших органов аудита, так и государственного сектора в целом. Как правило, государственные органы пользуются услугами внешних экспертов и/или высших учебных заведений для обучения сотрудников в формате мастер-классов, семинаров, корпоративных программ. Так, в рамках повышения цифровой грамотности сотрудников ВОА Ирана провел пятидневную Международную онлайн-программу по IT-аудиту (International Training Course on IT Audit) в период с 17 по 21 января 2022 г. В качестве спикеров были приглашены представители научного сообщества и практики в области ИТ-аудита.

Пандемия COVID-19 и необходимость организации удаленной работы органов государственной власти, включая ВОА, стали важным фактором для активизации процесса обучения сотрудников навыкам работы с цифровыми продуктами, в том числе и в удаленном формате. С начала пандемии все большую популярность набирает использование в процессе повышения квалификации сотрудников цифровых систем управления обучением (Learning Management System, LMS). Еще в 2005 г. Центр образовательных исследований и инноваций ОЭСР (Centre for Educational Research and Innovation, CERI) опубликовал исследование «Онлайн-обучение в сфере высшего образования» (E-Learning in Tertiary Education), в котором авторы определили LMS как программное обеспечение, предназначенное для предоставления ряда административных и педагогических услуг (например, данные о зачислении, доступ к электронным материалам курса, взаимодействие преподавателей и студентов, оценка и т.д.). За период с 2005 по 2022 гг. системы LMS превратились из административного инструмента в полноценную платформу для предоставления образовательных услуг в дистанционном формате.

Сегодня международные организации и ВОА могут не только разрабатывать свои платформы, но и покупать уже готовые (т.н. «коробочные») решения. Наиболее популярные из доступных LMS приведены на графике ниже.



Источник: Опрос Capterra, 2018 г., «Двадцать самых популярных LMS платформ» https://www.capterra.com/infographics/most-popular/learning-management-system-software/

Многие международные организации и ВОА предпочитают платформу Moodle (например, Учебный и научно-исследовательский институт ООН (United Nations Institute for Training and Research (UNITAR)), Структура ООН-женщины (UN Women), Инициатива развития ИНТОСАИ (INTOSAI IDI), Африканская организация высших органов аудита англоговорящих стран (АФРОСАИ-Е), Тихоокеанская ассоциация высших органов аудита (ПАСАИ), Академия Европейской счетной палаты (E-Academy of the European Court of Auditors)).

LMS содержат множество больших данных, которые могут помочь пользователю оценить дизайн курса электронного обучения. Например, процент завершения курса показывает, как продвигаются учащиеся и полностью ли они вовлечены в процесс обучения, а рейтинги удовлетворенности показывают, как учащиеся относятся к контенту, онлайн-инструкторам. Эти показатели LMS дают возможность оценить каждый аспект стратегии онлайн-обучения и разработать измеримые цели. Некоторые решения LMS имеют настраиваемые отчеты, которые позволяют отслеживать «болевые точки» онлайн-курсов для достижения желаемых результатов. В частности, важным показателем являются результаты прохождения курсов и успеваемость. К примеру, если половина учащихся не могут эффективно пройти курс на соответствие требованиям, это может указывать на то, что создателю нужно внимательнее выяснить корень проблемы, после чего изменить содержание обучения.

Тем не менее ключевой проблемой организации обучения на платформах LMS остается отсутствие адекватной проверки полученных знаний и, как следствие, полноценной сертификации, подтверждающей уровень освоения сотрудником необходимых компетенций. Дополнительная сложность возникает с авторскими правами в случае создания материалов несколькими авторами.

Кейсы

ВОА	**Национальное контрольно-ревизионное управление Великобритании (UK National Audit Office)**
Название	**Паспорт навыков (Skills passport)**
Дата	**21/06/2019**
Ссылка	

Вопрос контроля полученных знаний и измерения уровня цифровой грамотности и компетенций сотрудников государственных органов власти (включая ВОА) остается одним из приоритетов в рамках цифровой трансформации государственного управления. Национальное контрольно-ревизионное управление Великобритании, внедрило «Паспорт навыков» (Skills passport), в котором инспекторский состав на постоянной основе заполняет форму с указанием степени ознакомления с конкретной технологией или аналитическим методом проведения проверки.

ВОА	**Управление Генерального аудитора Дании (Auditor General Office of Denmark)**
Название	**Центр передового опыта в области анализа данных (In-House Center of Excellence for Data Analytics)**
Дата	**15/01/2020**
Ссылка	

В ВОА Дании создан Центр передового опыта в области анализа данных (In-House Center of Excellence for Data Analytics). Сотрудники центра помогают аудиторам в проведении контрольных мероприятий с использованием новых инструментов анализа данных. Важно отметить, что Дания дважды занимала первое место среди стран – членов ООН по уровню развития электронного правительства (UN E-Government Surveys).

ВОА	**Европейская счетная палата (European Court of Auditors)**
Название	**Руководящий комитет по цифровым технологиям (Digital Steering Committee)**
Дата	**2017**
Ссылка	

В рамках Европейской счетной палаты (European Court of Auditors, ECA) был создан Руководящий комитет по цифровым технологиям (Digital Steering Committee), в рамках которого функционирует ECALab – пространство для обмена идеями, изучения, тестирования и внедрения технологий в процесс аудита. Основными направлениями работы платформы являются использование инструментов анализа данных, визуализации и контроля процесса проведения проверок.

ВОА	**Национальное контрольно-ревизионное управление КНР (National Audit Office of China)**
Название	**Государственный аудит в условиях использования больших данных (National audit under the big data environment)**
Дата	**20/03/2018**
Ссылка	

Государственное контрольное управление Китайской Народной Республики (ВОА КНР) по результатам проводимого исследования обращает внимание на существование фактора сопротивления аудиторов изменениям. В настоящее время ВОА КНР продвигает комплексный подход к проведению аудита с использованием цифровых технологий, включающий общий анализ, выявление рисков и подозрительных действий, децентрализованную проверку и системные исследования. Аудит с использованием анализа больших данных подтверждает свою эффективность на практике, а также способствует изменению отношения к цифровым инструментам со стороны участников контрольных мероприятий.

ВОА	**Управление Генерального аудитора Непала (Office of the Auditor General)**
Название	**Цифровая система управления аудитом (Nepal Audit Management System)**
Дата	**26/01/2022**
Ссылка	

ВОА Непала запустил Цифровую систему управления аудитом (Nepal Audit Management System). Проект направлен на оптимизацию процесса аудита возможных рисков. Этапы проведения аудита, поддерживаемые программой, включают в себя:

- Планирование аудита с учетом рисков;
- Онлайн-доступ к объекту аудита;
- Механизм контроля и обеспечения качества аудита в режиме онлайн;
- Онлайн-передача сформированных системой аудиторских отчетов;
- Архивирование полученных документов

ВОА	**Счетная палата Российской Федерации (Accounts Chamber of the Russian Federation)**
Название	**Цифровой Университет для сообщества ИНТОСАИ (Digital University for INTOSAI Community, U-INTOSAI)**
Дата	**12/04/2021**
Ссылка	

Счетная палата Российской Федерации в 2021 г. запустила Цифровой университет для сообщества ИНТОСАИ (U-INTOSAI), за основу которого был взят LMS-плагин для WordPress.

Образовательные материалы, опубликованные на платформе U-INTOSAI, отражают опыт международных организаций, академического и бизнес-сообществ, а также ВОА, что способствует обеспечению повышения потенциала и компетенций аудиторов будущего.

В настоящий момент платформа доступна на семи языках и объединяет более 1500 зарегистрированных пользователей из 196 стран мира. На платформе представлены электронные курсы и подкасты по широкому кругу актуальных для ВОА тем: ЦУР, государственное управление, информационные технологии и аналитика данных, менеджмент, «мягкие» навыки и пр.

В процессе реализации инициативы U-INTOSAI команда столкнулась с рядом сложностей по различным направлениям:

- Недоверие потенциальных стейкхолдеров к новой платформе и эффективности дистанционного обучения, в целом;
- Сложности с поиском образовательного контента, подходящего для развития необходимых сообществу навыков;
- Узкая направленность платформы, и, как следствие, невозможность проведения классических маркетинговых компаний по «раскручиванию» ресурса.

ВОА	**Счетная палата Чешской Республики (Czech Republic Supreme Audit Office)**
Название	**Проект по обмену контрольной информацией, практиками, рекомендациями по итогам аудита (Benchmarking Information Exchange Project, BIEP)**
Дата	**11/2017**
Ссылка	

ВОА Чехии запустил Проект по обмену контрольной информацией, практиками, рекомендациями по итогам аудита (Benchmarking Information Exchange Project, BIEP). Среди возможностей портала – обсуждение актуальных профессиональных вопросов, проведение сравнительного анализа методологических подходов и результатов аудита в различных областях.

Рубрикатор BIEP

Основная идея BIEP заключается в сравнении ключевых показателей эффективности (KPI) и конкретных национальных условий в разных странах. Области сравнения не ограничены. BIEP направлен на экономии времени и затрат на аудит.

2022

Счетная палата

Российской Федерации