



ВАЛЕРИЙ ГРИБАНОВ,
РЕДАКТОР BUSINESS GUIDE
«ЦИФРОВАЯ ЭКОНОМИКА»

ВАКУУМ КАК ШАНС ДЛЯ РАЗВИТИЯ

Эксперты говорят, что цифровизация российской экономики за последний год приостановилась. Процессы внедрения новых продуктов и программных решений идут — и даже, наверное, более интенсивно, чем в предыдущие годы, но пока это ситуация, про которую говорят: «Нужно бежать, чтобы оставаться на месте». Сейчас все усилия отечественной ИТ-отрасли направлены не на внедрение новых процессов и освоение новых секторов, а на замену импортных продуктов, ушедших с отечественного рынка в прошлом году. То есть, по сути, вся работа ведется для заполнения вакуума, образовавшегося из-за ухода западных компаний или сознательного решения властей избавиться от их продуктов (если говорить о госсекторе).

Отчасти эта приостановка, вероятно, отразится на темпах развития экономики (хотя на фоне других факторов, влияющих на данный показатель, эти величины, скорее всего, будут малозаметными). С другой стороны, поиск новых решений всегда ведет к прорывам и неординарным векторам развития. Так, собственно, было с цифровизацией банковской системы. По сути, выращенная на пустом месте, она, эта система, к началу двадцатых годов оказалась одной из самых передовых в мире.

Сегодня оказаться в мировом авангарде будет несоизмеримо сложнее, учитывая санкции и общую экономико-политическую обстановку, в которой оказалась Россия. Однако и опираться на песимистические прогнозы, вполне возможно, не стоит — по крайней мере в вопросах импортозамещения ИТ-решений. Несмотря на отток большого числа айтишников за границу, специалистов, сильных в этой сфере, в стране, к счастью, по-прежнему достаточно.



КОЛОНКА РЕДАКТОРА

ЗАТЯНУВШЕЕСЯ «ЗАТЯГИВАНИЕ ГАЕК»

УЖЕСТОЧЕНИЕ РЕГУЛИРОВАНИЯ СФЕРЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, НАЧАВШЕЕСЯ В 2022 ГОДУ, ПРОДОЛЖИТСЯ И В ТЕКУЩЕМ. ЭКСПЕРТЫ ОЦЕНИЛИ ПЛЮСЫ И РИСКИ ИЗМЕНЕНИЙ ДЛЯ БИЗНЕСА. ПОЛИНА МАКАРОВА

События февраля 2022 года и последовавшие за ними новые санкции в отношении России обострили вопрос информационной безопасности страны. Так, по данным опроса «СерчИнформ», в прошлом году более трети опрошенных компаний отметили рост числа внешних кибератак по сравнению с 2021 годом, 44% респондентов столкнулись с утечкой информации, 32% — с утечкой персональных данных. Кроме того, возникли сложности с оборудованием и ИТ-продуктами зарубежных компаний, приостановивших или прекративших работу в России.

Реакция российских властей на изменения геополитической ситуации не заставила себя долго ждать. Уже в марте 2022 года вышел указ президента РФ № 166. Документом запрещалось органам государственной власти, госкомпаниям и операторам критической информационной инфраструктуры использовать средства информационной защиты иностранного производства. В случае, когда заменить их отечественными аналогами нельзя, была дана возможность обосновать использование зарубежных ИТ-продуктов и согласовать его. Действовать такая процедура должна до 2025 года, после чего планируется полностью запретить инструменты ИБ из недружественных стран. Спустя месяц после первого указа последовал второй — № 250. Он ввел те же запреты, но для стратегических и системообразующих предприятий (по состоянию на апрель 2023 года их насчитывается почти 1,4 тыс.). Также, согласно указу, в компаниях должны появиться ИБ-подразделения, если их еще нет, а ответственность за принятые меры возлагается на руководителя компании.

БОЛЬШЕ ТРЕБОВАНИЙ И ОТВЕТСТВЕННОСТИ В целом информационная безопасность — широкий термин и состоит из множества федеральных законов и подзаконных актов, напоминает управляющий партнер Legal House Ольга Звагольская. Речь идет о федеральных законах «Об информации, информационных технологиях и о защите информации» (№ 149-ФЗ), «О коммерческой тайне» (№ 98-ФЗ), «О персональных данных» (№ 152-ФЗ), «О безопасности критической информационной инфраструктуры Российской Федерации» (№ 187-ФЗ), о Доктрине информационной безопасности РФ (Указ президента №646) и проч. Сегодня, по словам госпожи Звагольской, все наблюдаемые изменения — это в основном раскрытие на подзаконном уровне ранее принятых положений федерального законодательства.

Все они так или иначе затрагивают бизнес. Довольно много нововведений вступили в силу в марте 2023 года. Так, теперь вместо 10 дней, в течение которых компании обязаны были уведомлять Роскомнадзор об изменении персональных данных, это необходимо сделать не позднее 15-го числа месяца, следующего за месяцем, когда произошли изменения. Также изменились правила уничтожения персональных данных. По словам экспертов, теперь компания должна подтверждать это актом об уничтожении личных данных и выгрузкой из журнала регистрации событий в информационной системе персональных данных. При этом если раньше акт об уничтожении можно было составить в свободной форме, то теперь есть перечень данных, указывать которые обязательно.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ



СЕГОДНЯ БОЛЬШЕ ВСЕГО ФИНАНСИРУЮТ ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ В НЕФТЕГАЗОВОЙ И ФИНАНСОВОЙ СФЕРЕ

Еще один важный мартовский приказ Роскомнадзора — № 178, отмечает Ольга Минаева, GR-директор «СерчИнформ». В нем впервые установлены критерии оценки размера вреда, нанесенного в результате утечки данных. «В рамках ожидаемого в 2023 году закона об оборотных штрафах такая оценка необходима для градации мер наказания для операторов персональных данных. Диверсифицированный подход позволит сформулировать осязаемое и соответствующее ущербу наказание за крупные утечки, особенно в части чувствительных данных», — отмечает госпожа Минаева.

Также в марте вступила в силу вторая часть масштабной реформы законодательства по обработке персональных данных. В частности, стали действовать нормы, регулирующие трансграничную передачу персональных данных. То есть компании должны уведомлять Роскомнадзор о зарубежных поставщиках, которые получают доступ к личным данным россиян. При этом, как поясняет госпожа Звагольская, ведомство может запретить такую передачу данных, ссылаясь в том числе на защиту основ конституционного строя и обеспечение обороны страны.

Вместе с ростом требований ужесточается и ответственность. Так, станет больше выездных проверок, связанных с персональными данными. При этом, как отмечают эксперты, по ряду нарушений привлечь к ответственности смогут и без контрольных мероприятий — для этого достаточно будет жалобы или информации в СМИ об утечке данных.

Вступившие в феврале этого года поправки в КоАП РФ устанавливают ответственность за подключение точки связи к точке обмена трафиком, владелец которой не обеспечивает реализацию установленных требований федерального законодательства. «На юридических лиц может быть наложена

ответственность до 300 тыс. рублей, или даже административное приостановление деятельности на срок до 90 суток (№ 19-ФЗ)», — уточняет Ольга Звагольская. Ольга Минаева напоминает, что сейчас обсуждается вопрос о введении уголовной ответственности за продажу персональных данных. «Конечно, здесь важно будет соблюсти баланс, провести качественное расследование и отследить всю цепочку участников, а не просто наказывать самого продавца как конечное физическое лицо», — надеется госпожа Минаева.

ПЛЮСЫ И РИСКИ Наблюдаемое сегодня ужесточение регуляторики в ближайшее время продолжится, считают эксперты. «Нас ожидает дальнейшее „затягивание гаек“, введение дополнительной ответственности, ужесточение ее. Государство непрозрачно намекает на токсичность любой трансграничной активности, а также на обязательность для бизнеса регулирования, связанного с информационной безопасностью», — говорит Ольга Звагольская. При этом, по ее словам, можно надеяться и на дальнейшее появление механизмов, способных помочь бизнесу исполнить новое регулирование и обеспечить безопасность собственной операционной деятельности. При этом она отмечает такую особенность текущего правового поля, как непредсказуемость изменений. «Может быть „воскрешен“ и принят одним днем законопроект, в течение многих лет находящийся на рассмотрении, при этом широко анонсированные нормы могут быть и не приняты. Широко распространена также практика „теневых поправок“, когда важные изменения какого-либо законодательного акта появляются во втором-третьем чтении какого-либо законопроекта, никак не связанного с предметом правок», — комментирует госпожа Звагольская.