

КРИТИЧЕСКИ ЗНАЧИМОЕ ИМПОРТОЗАМЕЩЕНИЕ

В НОЯБРЕ ДОЛЖНЫ БЫТЬ УТВЕРЖДЕНЫ ОКОНЧАТЕЛЬНЫЕ СРОКИ ПЕРЕХОДА НА ПРЕИМУЩЕСТВЕННОЕ ИСПОЛЬЗОВАНИЕ ОТЕЧЕСТВЕННОГО СОФТА И ОБОРУДОВАНИЯ НА ОБЪЕКТАХ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ (КИИ), КОТОРЫЕ ДОЛГОЕ ВРЕМЯ СЛУЖИЛИ ПРЕДМЕТом ДИСКУССИЙ В ОТРАСЛИ. ИСПОЛЬЗОВАНИЕ ЛОКАЛЬНЫХ ТЕХНОЛОГИЙ НА ЗНАЧИМЫХ ДЛЯ СТРАНЫ IT-СЕТЯХ — МИРОВОЙ ТРЕНД, ВАЖНЫЙ ДЛЯ ОБЕСПЕЧЕНИЯ ТЕХНОЛОГИЧЕСКОГО СУВЕРЕНИТЕТА. СЕГОДНЯ ЗАВИСИМОСТЬ ОТ ЗАПАДНЫХ ТЕХНОЛОГИЙ В РОССИИ В НЕКОТОРЫХ ОТРАСЛЯХ ВСЕ ЕЩЕ ДОСТИГАЕТ 100%, ХОТЯ ОТЕЧЕСТВЕННЫЕ РАЗРАБОТЧИКИ УЖЕ ГОТОВЫ ПОКРЫТЬ БОЛЬШУЮ ЧАСТЬ ПОТРЕБНОСТЕЙ ЗАКАЗЧИКОВ. ЮЛИЯ СТЕПАНОВА



СТРАТЕГИЧЕСКИ ВАЖНЫЕ ПРЕДПРИЯТИЯ СТРАНЫ ГОТОВЯТСЯ ПЕРЕВОДИТЬ СВОЮ ИНФРАСТРУКТУРУ НА ОТЕЧЕСТВЕННЫЕ IT-РЕШЕНИЯ

В ПОИСКАХ КОМПРОМИССА Правительство в ноябре должно утвердить сроки перехода на преимущественное использование отечественного программного обеспечения (ПО) и программно-аппаратных комплексов (ПАК) на объектах КИИ. «В результате долгих дискуссий мы с Минцифры пришли к компромиссу — январь 2023 года», — рассказала председатель правления Ассоциации разработчиков программных продуктов (АРПП) «Отечественный софт» Наталья Касперская. Ранее в проекте указа президента, который был представлен для общественного обсуждения, устанавливалось требование по преимущественному использованию отечественного ПО и ПАК на объектах КИИ до 2024 года для ПО, до 2025 года — для оборудования.

К объектам КИИ относятся: госорганы, банки, объекты транспорта, связи, здравоохранения, предприятия оборонной, топливной и атомной промышленности и энергетики. Их IT-сети считают критически важными для страны. Понятие «значимые объекты КИИ» появилось в 2018 году со вступлением в силу федерального закона 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», разработанного Федеральной службой по техническому и экспортному контролю (ФСТЭК). Этот

закон определяет регулирование защиты объектов КИИ, необходимость которого стала очевидной после масштабной атаки вируса WannaCry в 2017 году. Ликвидация последствий атаки обошлась каждой зараженной госкомпании от 3 млн до 5 млн руб. без учета стоимости восстановления программного обеспечения и информации.

Перейти на преимущественное использование отечественного софта для обеспечения технологической независимости и безопасности объектов КИИ поручил президент Владимир Путин 3 июля 2019 года. Исполняя поручение, ФСТЭК предлагала полностью отказаться от иностранных IT-решений на объектах КИИ. В проекте указа президента, разработанного Минцифры, говорится, что при наличии выбора между российским и иностранным продуктом приоритет должен отдаваться отечественному. Разработка нормативно-правовых актов, устанавливающих требования, процедуру и сроки импортозамещения на объектах КИИ, также есть во втором пакете мер поддержки IT-отрасли, который правительство утвердило 9 сентября. Ответственными по этому пункту являются Минцифры России, ФСТЭК России, ФСБ России, Минпромторг России.

Указанные в проектах нормативно-правовых актов сроки перехода стали предметом дискуссии

в отрасли. Отсрочка привела бы к тому, что все предприятия, которые относятся к КИИ, «просто выбросили бы эту проблему из головы», полагает Наталья Касперская. «Делать все в последний момент — наша национальная черта, и до начала 2023 года остается не так много времени, поэтому мне кажется, что Минцифры должно начинать заниматься проверками перехода на отечественные решения уже сейчас», — рассуждает она. В противном случае, по мнению Натальи Касперской, «к 2023 году мы окажемся ровно в том же самом положении, что и к концу 2021-го — когда выяснилось, что большинство предприятий не сделало никаких шагов в этом направлении».

ПРОБЛЕМА БЕЗОПАСНОСТИ ЗНАЧИМЫХ СЕТЕЙ Любая лакуна в технологическом стеке страны — готовая дыра для влияния, закладок, вторжения, а также возможность отключения извне теми, кому принадлежит технология или решение, говорит глава АРПП Наталья Касперская. Для субъектов КИИ, в частности, чужое влияние недопустимо, поскольку оно означает нарушение работы предприятий в стратегически важных областях, подчеркивает она. «Чтобы подобного не случилось, России нужно самостоятельно определять свою политику в технологическом пространстве», — полагает эксперт. Пока, по мнению Натальи Касперской, мы слишком сильно зависим от иностранных технологий: «Очень долго у нас системно внедрялись западные решения, и в результате в некоторых областях зависимость достигает 100%». При этом США ужесточают технологическую политику в отношении России, и некоторые эксперты уже прогнозируют возможность полного запрета ввоза высоких технологий в Россию, отмечает Наталья Касперская: «Мы должны быть готовы к такому сценарию, и последовательное импортозамещение — единственно возможная политика».

РОССИЙСКАЯ АЛЬТЕРНАТИВА Использование локальных технологий в элементах критической информационной инфраструктуры является современным трендом не только в России, но и за рубежом, например в США и Китае, говорит партнер департамента управления рисками Deloitte Сергей Кудряшов. При этом, в отличие от США или Китая, в России пока нет такого спектра отечественного оборудования и программных продуктов, которые полностью заместят иностранные аналоги, полагает он.

Противники импортозамещения часто говорят о том, что в нашей стране якобы нет российских продуктов, которые могут сравниться по качеству и функционалу с иностранными, но это не так: в стране есть аналоги практически всех западных программных продуктов, возражает Наталья Касперская. В реестре отечественного ПО сейчас более 11 тыс. наименований отечественных продуктов, подчеркивает она. По ее словам, комитет по интеграции отечественного ПО АРПП «Отечественный софт» ведет большую работу по созданию интегрированных решений компаний-членов для разных отраслей. «Интеграция означает, что программные продукты участников проходят тестирование на совместимость между собой», — поясняет Касперская. Таких пакетов у членов Ассоциации сейчас около четырех десятков, их количество постоянно растет, а также, добавляет эксперт, компаний — члены АРПП разрабатывают множество российских решений разных классов для субъектов КИИ — сейчас их более 150, и они покрывают практически все отрасли экономики.

Сложности могут возникнуть с переводом промышленных систем на отечественные аппаратные платформы к 2024 году — в пандемию рынок полупроводников столкнулся с невиданным кризисом, что прямо повлияло на сроки поставки и отгрузки оборудования с заводов — поставщиков комплектующих, объясняет директор по безопасности «МойОфис» Александр Буравцов. Дефицит компонентов распространяется на всех производителей оборудования, в том числе зарубежных, и если мы будем корректировать срок перехода на российские решения, это усугубит проблему, считает исполнительный директор Ассоциации российских разработчиков и производителей электроники Иван Покровский. По его оценке, в 2022 году проблема дефицита компонентов уже сойдет на нет.

Сроки перехода КИИ на российское оборудование могут быть и более ранними, считает Иван Покровский. По его словам, российские производители софта и оборудования уже закрывают многие потребности крупных компаний. Пока они не могут обеспечить высокопроизводительные вычислительные системы, телеком-оборудование с высокими требованиями к скоростям передачи данных, системы компьютерного зрения на основе искусственного интеллекта. «Но эти решения разрабатываются», — добавляет господин Покровский. КИИ необходимо обеспечить собственную полную технологическую цепочку, начиная от микропроцессоров и заканчивая прикладным ПО, заключает Наталья Касперская. ■