Почему импортозамещение может снизить угрозы кибербезопасности на объектах критической информационной инфраструктуры | 14

Review

Тематическое приложение к газете **Коммерсантъ**

Российский софт для значимой инфраструктуры

АРПП Отечественный софт

ГЕНЕРАЛЬНЫЙ ПАРТНЕР ВЫПУСКА

Вторник 23 ноября 2021 №212 (7174 с момента возобновления издания) **kommersant.ru**

15 | Как российские IT-компании справляются с дефицитом квалифицированных кадров

16 | Почему цифровизация госсектора способствует развитию отечественного IT-рынка в ближайшие годы

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.

ЮРИЙ МАРТЬЯНОВ

— правила игры —

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. В мае 2020 года Минцифры опубликовало для обсуждения проекты указа президента и постановления правительства о переходе владельцев КИИ на преимущественное использование отечественного ПО с 2021 года, а на российское оборудование — с 2022 года. В ответ на это финансовые организации заявили, что такие сроки перехода ставят под угрозу стабильность их работы и оказания услуг, а Ассоциация банков России обратилась к председателю правительства Михаилу Мишустину с просьбой отсрочить переход на четыре года.

Минцифры после обсуждений доработало проекты и сдвинуло сроки перевода КИИ на отечественные решения с 2024 и 2025 года для софта и железа соответственно. Такая мера вызвала недовольство IT-ассоциаций отечественных решений: за три года зависимость российских компаний от зарубежного софта и электроники только усилится, следует из письма АРПП «Отечественный софт» и Ассоциации российских разработчиков и производителей электроники, направленного в ноябре 2020 года президенту. Банки в то же время также остались недовольны инициативой Минцифры, заявив, что на переход им нужен срок как минимум до 2027–2028 годов.

В январе 2021 года в очередной версии проекта указа президента и постановления правительства Минцифры определило сроки перехода до 1 января 2023 года для софта и до 1 января 2024 года — для оборудования. В июне на форуме ITSF-2021 в Казани заместитель главы Минпромторга Василий Шпак заявил о том, что срок будет единым: «И ПО, и оборудование для КИИ будут российскими с 1 января 2023 года. Об этом на площадке правительства мы договорились с Минцифры».

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».

Важность перевода объектов КИИ на российское ПО и системы защиты обоснована также резким увеличением числа инцидентов информационной безопасности, считает директор по безопасности «МойОфис» Александр Буравцов. Так, в первой половине 2021 года в России было зафиксировано почти в три раза больше атак на объекты критической инфраструктуры, чем за весь 2019 год, сообщала Group-IB.

При грамотном выборе решений и их аккуратном и плановом внедрении защищенность объектов КИИ можно повысить, полагает Александр Буравцов. По его словам, основная проблема иностранных средств защиты и прикладного ПО в том, что у пользователей нет возможности точно определить наличие закладок и скрытых каналов управления. Проверку исходного кода на отсутствие недекларированных вендором возможностей обеспечивает процесс сертификации во ФСТЭК и других органах технического контроля, отмечает эксперт. Вендор сертифицированного ПО обязан отслеживать и оперативно устранять выявленные уязвимости в своем и стороннем коде, информировать пользователей об обновлениях, развивать решение, продлевать сертификаты соответствия. Приобретение сертифицированного решения — это уверенность в том, что за безопасность данных в случае какого-либо инцидента отвечает вендор приобретенного ПО, подчеркивает господин Буравцов.

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, компании—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 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.

Юлия Степанова

Аппаратуру загрузят по-русски

— регулирование —

Долгое время разработки отечественного программного обеспечения (ПО) и российской электронно-компонентной базы шли параллельно, и за эти направления в части импортозамещения отвечали два разных министерства — Минцифры и Минпромторг. Несогласованность политики в части господдержки этих секторов привела к тому, что многие российские софтверные решения были не адаптированы для работы на российских процессорах, что осложняло создание полностью отечественных программно-аппаратных комплексов. Но сейчас ситуация меняется: министерства объединяют действия в части поддержки разработчиков, а участники рынка начали создавать коллаборации, которые уже вылились в комплексные решения.

Усиление в команде

В текущем году власти начали вести планомерную работу по гармонизации политики в части импортозамещения софта и программно-аппаратных комплексов (ПАК), а также озаботились вопросом их совместимости с отечественным программным обеспечением. Первым шагом в этом направлении стало наделение Минцифры новыми полномочиями по стимулированию спроса на «отечественную радиоэлектронную продукцию, ПАК и программное обеспечение». Министерство будет отвечать за прогнозирование спроса на радиоэлектронику, выработку мер господдержки, вопросы повышения конкурентоспособности российской продукции. Одним из возможных шагов по формированию спроса может стать установление приоритетов для оборудования и ПАК российской разработки в национальной программе «Цифровая экономика Российской Федерации» (ЦЭ). Наибольшим потенциалом с точки зрения спроса обладает федеральный проект «Информационная инфраструктура», на его реализацию планируется потратить 768 млрд руб. до 2024 года.

Минцифры также сможет заключать от имени РФ специнвестконтракты, контролировать их исполнение, согласовывать графики закупок госорганами гражданской радиоэлектроники и ПАК, а также определять условия допуска к госзакупкам иностранной продукции. Также к нему перейдет разработка критериев для признания компаний разработчиками отечественной продукции, чтобы они могли претендовать на госфинансирование проектов и льготы. До этого критерии отечественной электроники разрабатывал Минпромторг, он отвечает за ведение реестра, на который должны ориентироваться при закупках госкомпании и госзаказчики. Минцифры ведет реестр отечественного софта.

Минпромторг со своей стороны также делает шаги по стимулированию разработки ПАК на базе отечественного софта и железа. Еще летом министерство обратилось к российским разработчикам ПО с просьбой обеспечить совместимость их продуктов с российскими процессорами «Эльбрус» и «Байкал». В министерстве полагают, что эту работу нужно ускорить с учетом новых требований по импортозамещению. По прогнозу Минпромторга, к 2023 году не менее 70% закупаемой государством вычислительной техники будет на отечественных процессорах.

Синхронизация усилий

Проблема в том, что пока действительно многие российские софтверные решения не адаптированы для работы на российских процессорах. Но ситуация стремительно меняется. В июне разработчик отечественной операционной системы «Базальт СПО», МЦСТ (разрабатывает процессоры «Эльбрус»), «Байкал Электроникс», ЭОС (создает отечественное ПО для электронного документооборота) и «МойОфис» представили полностью импортонезависимое многоместное автоматизированное рабочее место (АРМ) для использования в МФЦ.

с 15

Софт поставят по подписке

— инновации —

К 2024 году в России может появиться модульная мультисервисная платформа промышленного софта, работающая по принципу маркетплейса. Идея в том, что предприятия, которым требуется инженерное программное обеспечение (ПО), смогут получать его по подписке, а вендоры получат доступ к единой среде разработки. Необходимость подобной платформы, по словам участников рынка, назрела давно. Она поможет решить проблему технологической зависимости в критической для оборонной промышленности сфере, выявит лидирующие решения и положительно скажется на популяризации российских программных продуктов, полагают эксперты.

Единая среда разработки

В октябре стало известно, что Минпромторг разработал «дорожную карту» по созданию единой экосистемы промышленного ПО. Такая экосистема должна работать по модели маркетплейса: в ней будут представлены программы, которые предприятия используют для управления производственными процессами, проектировки изделий, диспетчерского контроля, сбора данных с объектов и т. д. (EPR, MDM, MES, SCADA, PDM, САПР). Проект получил название «Модульная мультисервисная промышленная платформа» (ММПП). Пилотный запуск намечен на август 2022 года, а полностью завершить проект планируется в 2024 году. Предприятия, которым требуется инженерное ПО, смогут получить его на платформе по подписке, компенсировав часть затрат за счет субсидий.

Платформа станет «единой средой разработки и тиражирования российского инженерного и промышленного софта». Она призвана решить несколько вызовов и проблем, которые сейчас стоят перед отраслью. В их числе необходимость ускоренного импортозамещения, технологические и политические риски использования зарубежного софта и отсутствие на текущий момент так называемых сквозных архитектур на отечественном рынке. ММПП будет представлять собой комплекс взаимосвязанных и распределенных программно-технических средств, обеспечивающий взаимодействие большого количества участников путем использования на платформе единой среды разработки. В частности, система будет поддерживать единые форматы обмена данными и протоколы.

Сейчас Минпромторг обсуждает с отраслью, какие классы и типы программного обеспечения могут быть включены в платформу, возможность использования программного обеспечения с открытым кодом и коллективной (консорциумной) разработки, а также организационно-функциональную схему взаимодействия с потребителями.

Минпромторг также провел анкетирование 951 предприятия промышленности. Из исследования, проведенного по итогам опроса, следует, что отечественные ERP, MDM и MES наиболее конкурентоспособны из рассматриваемых продуктов. В отличие от них, российские системы класса DPM, PLM и SCADA менее востребованы. Это, по оценке министерства, обусловлено значимостью для потребителей сквозных решений, менее развитых в отечественном ПО.

Вызовы рынка

Инициатива Минпромторга может решить проблему технологической зависимости в критической для оборонной промышленности сфере, полагают эксперты. Задача перейти от фильтрующего реестра отечественного ПО к площадке, на которой ПО можно протестировать, посмотреть кейсы использования, оценить возможности интеграции и купить, давно назрела, считает директор технологической практики КПМГ в России и СНГ Сергей Вихарев.

«В ряде категорий промышленной автоматизации и промышленного интернета вещей отечественное ПО — это решения собственной разработки крупных корпораций, которые выводят его на открытый рынок в целях коммерциализации. Ясно, что такие решения пока не стали «коробочными» и в основном требуют значительной доработки под каждого конкретного заказчика». Отечественный маркетплейс, по мнению господина Вихарева, должен не столько упростить покупку лицензий, сколько стимулировать разработку интеграционных модулей для промышленных систем управления разных разработчиков.

Однако создание предложенной Минпромторгом платформы может столкнуться с рядом сложностей и вопросов, предупреждают разработчики. «При создании подобной системы необходимо будет проработать ответ на вопрос, какую добавленную ценность она несет в процессе цифровизации и цифровой трансформации конкретного предприятия»,— отметил гендиректор «Аскон» (российский разработчик инженерного ПО) Максим Богданов. Например, для каталогизации отечественного ПО создан соответствующий реестр, и пока не ясно, как платформа будет взаимодействовать с ним, говорит он.

с 15

Review **Российский софт для значимой инфраструктуры**

РЕДСОФТ TrueConf ОТКРЫТАЯ МОБИЛЬНАЯ ПЛАТФОРМА

Трубопроводы зависли на загрузке

Объекты критической информационной инфраструктуры страны, в числе которых госорганы, банки, промышленные предприятия и телекоммуникационные сети, все чаще становятся целями кибератак, и их число растет из года в год. Одна из наиболее острых проблем, которая сказывается на безопасности IT-контура таких структур,— несвоевременное обновление программного обеспечения и использование зарубежных решений, которые могут иметь уязвимости. Импортозамещение, по словам экспертов, может снизить угрозы, исключив риски технологической зависимости стратегически важных объектов. Но отечественные решения при этом должны соответствовать высоким требованиям в части информационной безопасности.

— безопасность —

В текущем году рост числа хакерских атак на стратегические предприятия России ускорился, отмечают эксперты по информационной безопасности. К таким объектам относятся госорганы, банки, предприятия оборонной промышленности, объекты транспорта, здравоохранения и др. Злоумышленники, как правило, пытаются завладеть почтой топ-менеджеров предприятий и перехватить контроль над инфраструктурой.

Так, по данным отчета Kaspersky ICS CERT, в первом полугодии 2021 года доля атак шпионского ПО и вредоносных скриптов на компьютеры автоматизированной системы управления техпроцессов (АСУ ТП), которые используются в промышленности, составила 33,8% в мире и 39,4% в России — на 4,8 п. п. больше по сравнению с прошлым полугодием. Такой рост вывел Россию на пятое место среди регионов мира по этому показателю после Африки, Юго-Восточной и Центральной Азии. Всего в первом полугодии компания зафиксировала в системах промышленной автоматизации более 20 тыс. модификаций вредоносного ПО из 5 тыс. различных «семейств».

Все угрозы, по оценке экспертов, увеличились на 4,8 п. п., до 39,4%. Среди исследованных индустрий наибольший процент атакованных компьютеров АСУ ТП зафиксирован в машиностроении (53,7%), а наименьший — в нефтегазовой отрасли. Основными источниками угроз для компьютеров в технологической инфраструктуре организаций остаются интернет, съемные носители и электронная почта.

Госсектор под прицелом

Кроме того, растет число целенаправленных атак. Такие атаки обычно хорошо спланированы и включают несколько этапов: от разведки и внедрения до уничтожения следов присутствия. Как правило, в результате целенаправленной атаки злоумышленники закрепляются в инфраструктуре жертвы и остаются незамеченными в течение месяцев или даже лет — на протяжении всего этого времени они имеют доступ ко всей корпоративной информации.

Так, в сентябре эксперты по кибербезопасности обнаружили новую хакерскую группировку ChamelGang, которая атакует учреждения в десяти странах мира, в том числе в России. С марта под прицел попали отечественные компании в топливно-энергетическом комплексе и авиапроме, как минимум две атаки оказались успешными. Жертвами по всему миру также стали учреждения Индии, США, Тайваня и Германии. Злоумышленников интересуют данные из скомпрометированных сетей, полагают эксперты.

Хакеры маскируют вредоносное ПО и сетевую инфраструктуру под легитимные сервисы. Например, они регистрируют фишинговые домены, имитирующие сервисы поддержки, доставки контента и обновлений Microsoft, TrendMicro, McAfee, IBM, Google и других компаний. Среди инструментов группировки в том числе новое, ранее не описанное вредоносное ПО ProxyT, BeaconLoader и бэкдор DoorMe, то есть лазейка, которая позволяет хакеру получить доступ в систему, выяснили в Positive Technologies.

Ранее, в сентябре, британская компания по информационной безопасности Cyjax обнаружила масштабную атаку против сотрудников госорганов России и соседних государств. Злоумышленники создают сайты, имитирующие вход в электронную почту для чиновников, а данные могут использовать для дальнейшей атаки на ведомства или продажи доступа на теневом рынке. Среди атакуемых организаций — Российская академия наук, почтовый сервис Mail.ru, а также госструктуры более десятка стран, включая Армению, Азербайджан, Китай, Киргизию, Грузию, Белоруссию, Украину, Турцию, Туркмению и Узбекистан. Компания проанализировала более 50 доменов в рамках этой схемы и выяснила, что они стали появляться еще с весны 2020 года.

Годом ранее «Лаборатория Касперского» зафиксировала серию целевых атак на российские организации сферы здравоохранения. По данным компании, весной и в начале лета 2019 года были атакованы до десяти крупных государственных учреждений в южных регионах России. На тот момент экспертам не удалось выяснить, кто стоит за атаками, но они отметили, что атакующие свободно говорят на русском языке, но территориально находятся за пределами страны.

В целом каждая десятая критически значимая информационная инфраструктура (КИИ) в России скомпрометирована вредоносом, обнаружили в «Ростелеком-Соларе». Хакерские группировки находят в софте российских объектов КИИ так называемые уязвимости нулевого дня (то есть неизвестные разработчикам), а затем пытаются взломать почтовые серверы и компьютеры первых лиц компаний и ведомств.

По оценке аналитиков, совершить атаки на их сети сейчас могут даже не слишком квалифицированные хакеры: проблема в том, что более 90% организаций своевременно не обновляют софт. Большинство промышленных объектов, например, работают с прикладными ПО, которые разрабатывались под старые версии операционных систем. Но в целом ситуация уже улучшается, считают эксперты, в том числе из-за изменений в законодательстве.

ДОЛЯ КОМПЬЮТЕРОВ СИСТЕМ ПРОМЫШЛЕННОЙ АВТОМАТИЗАЦИИ, НА КОТОРЫХ БЫЛИ ЗАБЛОКИРОВАНЫ ВРЕДОНОСНЫЕ ОБЪЕКТЫ В РАЗНЫХ ИНДУСТРИЯХ (%) ИСТОЧНИК: «ЛАБОРАТОРИЯ КАСПЕРСКОГО».

По ФЗ-187 «О безопасности критической информационной инфраструктуры», вступившему в силу в 2018 году, все объекты КИИ передают информацию об инцидентах в Государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак, созданную ФСБ. По закону за несоответствие требованиям регулятора вводится административная ответственность, а если незащищенность КИИ привела к серьезным последствиям, может последовать и уголовная.

Проблема уязвимости

Корпоративные данные — это товар, который всегда был объектом охоты для злоумышленников, но в связи с пандемией и переводом сотрудников на дистанционный режим за последние два года вектор хакерских атак изменился, отметил директор по развитию TrueConf Дмитрий Одинцов. Целью номер один для взломщиков, по его словам, стали персональные устройства сотрудников — слабо защищенные и не подготовленные к новой реальности. «Причин для роста атак хватает: компании игнорируют риски использования незащищенных сетевых подключений, не следят за выполнением регламентов доступа к корпоративным ресурсам, позволяют сотрудникам делиться конфиденциальной информацией и проводить рабочие встречи в публичных онлайн-сервисах. Также нельзя исключать человеческий фактор и банальную невнимательность»,— отмечает Дмитрий Одинцов.

Изначально сети объектов промышленной инфраструктуры создавались закрытыми, но со временем стали появляться соединения с внешними сетями, что снизило их безопасность, объясняет руководитель экспертного центра по промышленной кибербезопасности «Лаборатории Касперского» Антон Шипулин. В целом атаки на подобные объекты могут привести к остановке производства, рискам экологических катастроф и жизни людей, отмечает он.

Сейчас активнее всего растут атаки на промышленность с использованием вымогательского программного обеспечения, и сфера промышленности, по оценке «Лаборатории Касперского», больше других платит выкупы злоумышленникам. Недавний пример — майская атака программ-вымогателей на оператора американского трубопровода Colonial Pipeline. Хакерская атака вынудила Colonial Pipeline перекрыть жизненно важный трубопровод. Злоумышленники также украли данные компании — около 100 ГБ.

Частая проблема — несвоевременное обновление софта, которое необходимо для закрытия уязвимостей, которые могут эксплуатировать хакеры, подтверждает эксперт. Доля зарубежного софта, который может иметь уязвимости, в объектах критической информационной инфраструктуры России все еще велика, и 11 октября Совет безопасности обсуждал эту проблему, рассказал Антон Шипулин. Импортозамещение, по его мнению, может частично решить эту проблему, снизив риски технологической зависимости стратегически важных объектов от зарубежных решений. «Однако важно, чтобы отечественные решения соответствовали высоким требованиям в части информационной безопасности — в противном случае мы не решим проблему, а заменим уязвимый зарубежный софт на такой же, но российский»,— предупреждает он.

Отечественный софт закрывает пробел

В первую очередь защищенность данных определяется правильной корпоративной политикой в отношении информационной безопасности на предприятиях, отмечает Дмитрий Одинцов. «Традиционная особенность российского IT-ландшафта — это большое внимание к информационной безопасности. Отечественные антивирусы, криптографические шлюзы и серверные решения для видеосвязи можно без преувеличения назвать лучшими в мире»,— отмечает эксперт. Точно можно сказать: массовое внедрение таких продуктов в российских компаниях позволило бы минимизировать риски утечки данных даже в условиях удаленной работы, уверен он. Однако стопроцентную защиту от человеческого фактора такие продукты гарантировать не могут, признает Дмитрий Одинцов.

Корпоративные стандарты в отношении информационной безопасности в компаниях и организациях обязательно должны включать в себя долгосрочную стратегию по развертыванию и развитию доверенной, основанной на российских технологиях корпоративной мобильности, отмечает гендиректор компании «Открытая мобильная платформа» (ОМП) Павел Эйгес: «Ведь именно использование личных мобильных устройств в рабочих целях, а все они так или иначе контролируются зарубежными платформами и поставщиками, приводит к существенному увеличению поверхности атаки».

«То, что в повседневной жизни обеспечивает удобство и доступность использования цифровых сервисов, дает злоумышленникам возможность реализовывать атаки с использованием механизмов фишинга, социальной инженерии с утекшей персональной и корпоративной информации с мобильного телефона сотрудника»,— рассуждает Павел Эйгес.

Экспертиза ОМП как компании, которая специализируется на разработке корпоративной мобильной ОС «Аврора», показывает, что внедрение в организациях собственной доверенной мобильной платформы существенно снижает риски, отмечает Павел Эйгес.

Переход на отечественные решения, который уже происходит, позволяет не только исключить целый ряд уязвимостей в КИИ, но и привел к созданию центров компетенции по адаптации продуктов к новым вызовам, отмечает эксперт. «Но это, конечно, не отменяет требований конкурентоспособности и безопасности самих российских решений»,— подчеркивает он. Также важно, что речь идет о сотрудничестве и взаимодействии многих российских компаний, о целых экосистемах, говорит господин Эйгес: «Это объединение уже приводит к отличным результатам в реализованных проектах».

Юлия Тишина

ТЭК прокачал отечественную ОС

— внедрение —

Заместитель гендиректора отечественного поставщика IT-решений «РЕД СОФТ» РУСТАМ РУСТАМОВ о санкционной устойчивости в топливно-энергетическом комплексе (ТЭК) страны.

ПРЕДОСТАВЛЕНО «РЕД СОФТ»

В 2020 году «РЕД СОФТ» успешно завершила проект по внедрению российской импортонезависимой операционной системы (ОС) «РЕД ОС» в IT-инфраструктуру крымского «Черноморнефтегаза». Это крупное отечественное предприятие, основной сферой деятельности которого является разведка и разработка месторождений нефти и газа в Черном и Азовском морях. Как и другие государственные структуры, «Черноморнефтегаз» подпадал под действие нормативных актов о запрете на осуществление закупок программного обеспечения, происходящего из иностранных государств. При этом необходимость перехода на отечественный софт обострялась санкционной политикой западных вендоров, которая ставила под угрозу процессы предприятия.

К моменту начала работ по внедрению «РЕД СОФТ» уже обладала опытом в сфере импортозамещения, а «РЕД ОС» — широкой экосистемой совместимых продуктов, которая непрерывно развивалась. Разработка «РЕД ОС» ведется с 2014 года на базе Linux. Продукт зарегистрирован в Едином реестре российских программ для ЭВМ и баз данных и сертифицирован ФСТЭК России, что допускает его применение для защиты государственных информационных систем, систем персональных данных, критической информационной инфраструктуры и автоматизированных систем управления технологическим процессом до первого класса защищенности включительно.

У нас большое количество технологических партнеров, в числе которых производители «железа» и разработчики офисных приложений, решений в сфере информационной безопасности, систем электронного документооборота, специализированных решений и др. Соответственно, мы были готовы обеспечить совместимость как оборудования, так и программного обеспечения, используемого в «Черноморнефтегазе», с нашей ОС. По итогам проекта мы довели общий процент отечественного ПО в IT-инфраструктуре предприятия до установленных законодательством требований.

«Черноморнефтегаз» стал первым санкционным проектом для нашей компании, первым на территории Крыма и первым в ТЭКе. Перевод стратегического для жителей полуострова и для страны в целом нефтедобывающего предприятия преимущественно на российскую «РЕД ОС» с целым спектром сопутствующих продуктов позволил не только повысить независимость IT-инфраструктуры предприятия от иностранного программного обеспечения и связанных с его эксплуатацией рисков, но и обеспечить функциональность и удобство в использовании отечественного софта. Этот успешный опыт позволил нам продолжить работу в секторе. На данный момент мы сотрудничаем с ПАО «Транснефть», ПАО «Газпром», их дочерними структурами, а также с другими предприятиями ТЭКа.

«Мы активно следуем взятому страной курсу»

— экспертное мнение —

Директор по развитию TrueConf ДМИТРИЙ ОДИНЦОВ об импортозамещении решений для видеоконференцсвязи (ВКС) в государственном и корпоративном секторах.

ПРЕДОСТАВЛЕНО «TRUECONF»

— Пандемия спровоцировала массовый переход всех секторов экономики на удаленную работу. Как проходил этот процесс?

— Очень резко. Сразу же, как были анонсированы первые нерабочие дни в марте прошлого года, нагрузка у нас выросла более чем в 30 раз. Мы тогда приняли решение все корпоративные лицензии отдавать бесплатно, чтобы помочь экономике как можно быстрее наладить удаленную работу. Более 4 млн сотрудников разных ведомств и организаций стали нашими новыми пользователями в те недели, и это только в России.

— Изменилось ли отношение компаний к видеоконференциям?

— Скорее поменялось отношение у самих пользователей. Скепсис ушел, и они вдруг поняли, что видеосвязь действительно позволяет работать и решать даже сложные задачи на расстоянии. И, конечно, самый лучший пример продемонстрировало наше правительство: каждый день на телеканалах показывают заседания по видеосвязи.

— О каких рисках идет речь при организации удаленных коммуникаций внутри предприятия?

— Как раз наоборот, если коммуникации происходят внутри предприятия — рисков минимум. А когда люди начали массово работать удаленно в незащищенных условиях, то выставили себя в роли слабого звена для злоумышленников. Возникло множество проблем, связанных с риском утечки данных или использованием неконтролируемых публичных сервисов для связи.

— Какие существуют механизмы устранения подобных рисков? Есть ли примеры подобных внедрений?

— Да, именно этим мы и занимаемся, помогая вернуть корпоративные видеокоммуникации под контроль. Достигается это за счет установки собственной защищенной системы ВКС и применения современных протоколов связи. Все крупнейшие российские компании уже давно идут по этому пути. За границей IT-департаменты в госсекторе, силовых структурах и промышленности думают так же.

— Как относятся к российскому ПО для видеосвязи заказчики на Западе?

— В целом очень лояльно. Российское ПО — это признак качества, что в нашем случае регулярно подтверждается наградами от мировых аналитических агентств Gartner и IDC и растущей долей экспорта по всему миру. Даже в США, несмотря на политический климат, широко применяются решения TrueConf.

— В России пока используется много иностранных аппаратных решений. Готовы ли мы к импортозамещению?

— Готовы и уже активно следуем взятому страной курсу, о чем говорят тысячи отгруженных отечественных ВКС-терминалов. По отзывам специалистов, которые управляют крупнейшими парками таких устройств в стране, наши решения хорошо защищены и проще в администрировании, чем зарубежные.

Интервью взял Матвей Соколов

Критически значимая мобильность

— экспертное мнение —

Генеральный директор компании «Открытая мобильная платформа» ПАВЕЛ ЭЙГЕС о преимуществах использования доверенной мобильной операционной системы (ОС) «Аврора» на объектах критической информационной инфраструктуры (КИИ).

АЛЕКСАНДР КАЗАКОВ

— Каким образом ОС «Аврора» может повысить безопасность КИИ?

— Цифровизация всех областей экономики набирает обороты, выявляя важную проблему — отставание корпораций и госорганов от потребительского опыта сотрудников, который зачастую превалирует над требованиями к функциональности и информационной безопасности. Так, например, желание использовать личные мобильные устройства для решения рабочих задач приводит к утечкам информации.

В то же время текущие геополитические изменения вместе с возможностью зарубежных производителей оказывать влияние на использование в России их аппаратных и программных продуктов повышают технологические и экономические риски отдельных отраслей и страны. Очевидно, что в такой ситуации требуется собственная доверенная платформа, включающая уровень аппаратного обеспечения, уровень ОС и системного ПО, приложений, сервисов и инфраструктуры. Мобильная ОС «Аврора», платформа управления мобильными устройствами и приложениями «Аврора Центр», доверенная среда исполнения «Аврора ТЕЕ» — та основа, которая позволяет строить решения бизнес-задач с использованием отечественных технологий в строгом соответствии с требованиями регуляторов и текущей геополитической ситуацией.

— Как сейчас развивается экосистема на ОС «Аврора»?

— Сегодня на платформе «Аврора» выстроилась экосистема приложений — как встроенных, так и разработанных нашими партнерами. Мы делаем все для развития тиражного ПО и инвестируем в это. Все инструменты, необходимые разработчикам, мы предоставляем бесплатно.

— На каких устройствах и программно-аппаратных комплексах уже работает «Аврора»?

— На российских смартфонах и планшетах QTech, «Ф-Плюс», «Аквариус», MIG, «БайтЭрг», INOI, а также на новых отечественных аппаратных платформах «Скиф» и «Байкал-М».

— Какие сектора экономики могут перейти на использование доверенной мобильной платформы?

— Наши решения уже работают и активно внедряются на предприятиях топливно-энергетического комплекса, в нефтегазовой отрасли, на транспорте, в государственных компаниях и, конечно, на объектах КИИ. Везде, где требуется независимая доверенная мобильная платформа на стеке отечественных технологий. Зачастую платформа «Аврора» позволяет мобилизовать бизнес-процессы там, где это ранее было невозможно из-за требований безопасности или регуляторики.

Интервью взял Матвей Соколов

Review

Российский софт для значимой инфраструктуры

COMMUNIGATE SYSTEMS

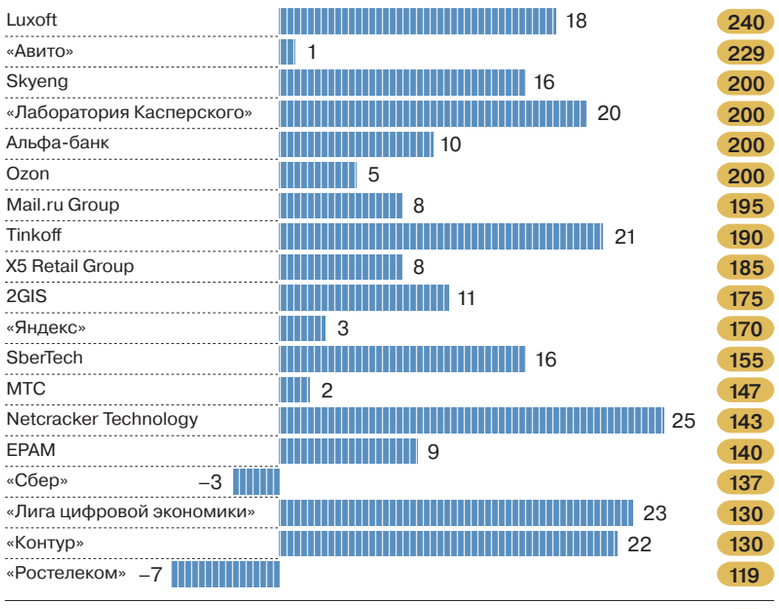
Раскадровка в IT

В сфере информационных технологий нехватка специалистов была всегда, но на фоне пандемии и ускоренной цифровизации кадровый голод усилился. При этом он касается в основном высококвалифицированных сотрудников уровней senior и middle. Наиболее остро этот вопрос стоит на объектах критической информационной инфраструктуры (КИИ), поскольку к специалистам в таких секторах предъявляются специфические требования как в части информационной безопасности, так и знания законодательства.

— правила игры —

ДИНАМИКА МЕДИАНЫ ЗАРПЛАТЫ IT-СПЕЦИАЛИСТОВ В РОССИЙСКИХ КОМПАНИЯХ (% — РАЗНИЦА ПЕРВОГО ПОЛУГОДИЯ 2021 ГОДА СО ВТОРЫМ ПОЛУГОДИЕМ 2020 ГОДА)

ИСТОЧНИК: «ХАБР КАРЬЕРА».



Массовый переход на удаленные решения, ускоренная цифровизация и меры господдержки стали катализаторами спроса на IT-специалистов. Разработчики софта в текущем году были вынуждены поднять цены на свои продукты больше, чем обычно,— на 20%, объясняя это ростом зарплат программистов (см. „Ъ“ от 29 сентября). При этом требования к IT-специалистам за пандемию не изменились, но изменились требования специалистов к компаниям, говорит продакт-менеджер «Хабр Карьеры» Артем Зыза. Шутка «Долго не собеседуйте программиста, потому что к концу собеседования кандидат дорожает» уже не шутка, замечает директор по росту Bi.Zone Рустэм Хайретдинов. Если раньше разрыв в зарплате разработчиков при переходе в другую компанию составлял 5–10%, то сейчас он доходит до 50%, писал „Ъ“ в июле. Для поиска IT-специалистов стали использоваться даже сервисы знакомств, а также появились приложения, которые работают по модели Tinder.

Пандемия подхлестнула цифровизацию, которая потребляет труд IT-специалистов, как топливо, говорит Рустэм Хайретдинов. За время пандемии количество российских компаний, которые предлагают удаленный или гибридный формат работы, увеличилось с 20% до 70%, говорит Артем Зыза. Снятые во всем мире ограничения на удаленку привели к тому, что за российских айтишников стали бороться не только отечественные, но и американские, европейские и китайские компании, отмечает Рустэм Хайретдинов. «Совершенно стандартной стала ситуация, когда IT-специалист может жить в небольшом сибирском городке и работать на крупнейшую американскую или китайскую компанию»,— рассказывает он.

Конкурентными преимуществами при выборе работодателя являются уровень оплаты труда, качество продуктов и услуг и современные подходы к управлению проектами, рассуждает директор по развитию персонала «Лиги цифровой экономики» Ангелина Капитонова. При этом по сравнению с Европой и США в России сейчас сильно завышены требования к экспертам — технические и в части возраста, опыта кандидатов, отмечает она. Чтобы остановить утечку мозгов, важно снижать требования, а бизнес-процессы выстраивать таким образом, чтобы иметь возможность дробить сложные задачи на мелкие, которые в состоянии решать сотрудники с не самой высокой квалификацией, полагает госпожа Капитонова.

Школьники выходят на поле

Чтобы смягчить дефицит кадров, отечественные разработчики стали чаще нанимать IT-специалистов из регионов. Так как меньше компаний стало требовать релокацию, возросла конкуренция между специалистами: если раньше им приходилось конкурировать только с ребятами из своего города, то теперь приходится активнее доказывать свою профпригодность, говорит ментор Solvery Азат Загитов.

Требования компаний к айтишникам даже снизились, чтобы хоть както заполнить горячие вакансии, возражает Рустэм Хайретдинов. После долгих поисков кандидата на старшую (senior) позицию компании часто берут средних (middle) специалистов с потенциалом, чтобы потом их обучить и дотянуть до необходимых требований, рассказывает он. Конкуренция за начинающих (junior) специалистов уже сместилась на первые курсы институтов и даже старшеклассников, добавляет эксперт. По прогнозу аналитиков в ближайшие несколько лет в отрасли будет примерно 40% программистов без высшего образования, окончивших лишь короткие курсы, добавляет она.

Раздувающаяся цена на IT-специалистов привлекает в эту отрасль новичков и вызывает рост числа курсов, которые «штампуют специалистов сомнительной ценности», говорит Азат Загитов. В результате дефицит на рынке касается именно качественных кадров — senior- и middle-специалистов, полагает он. Этому способствуют и действия компаний из регионов. Поскольку они не могут позволить себе повышение зарплат, то, чтобы удержать специалистов, компании вынуждены менять кадровую политику и повышать сотрудников, например, с позиции middle- до senior-специалиста. Спустя год такой senior-специалист выходит на рынок труда и просит зарплату вдвое или втрое выше, рассказывает Азат Загитов.

Организации, которые не способны конкурировать с крупнейшими международными компаниями по зарплате, прибегают и к нематериальным стимулам: предлагают свободный график, комбинированный режим работы, различные нерабочие игровые и спортивные активности, первоклассную технику для работы и другие виды мотивации, отмечает Рустэм Хайретдинов.

Специфика кадров для КИИ

Наиболее остро кадровый вопрос стоит на объектах критической информационной инфраструктуры. С января по середину октября нынешнего года на hh.ru были размещены 1,6 тыс. вакансий, в описании функционала которых есть упоминание взаимодействия с КИИ, рост к аналогичному периоду прошлого года составил два раза, рассказал директор департамента специальных проектов hh.ru Виталий Терентьев. При этом на hh.ru количество резюме соискателей с опытом взаимодействия с КИИ за неполный 2021 год составило также 1,6 тыс. Таким образом, соотношение спроса и предложения в данном сегменте рынка — один к одному, что является острым дефицитом.

Объекты КИИ предъявляют к кадрам наиболее высокие требования, что связано с высокой стоимостью ошибки на подобных объектах, говорит Артем Зыза. Специфическое требование к IT-специалистам объектов КИИ — знание российского системного и прикладного программного обеспечения, так как к 2023 году такие предприятия должны перевести свою цифровую инфраструктуру на российское ПО, уточняет генеральный директор ИВК Григорий Сизоненко: «Поэтому ценным становятся умение сотрудника сориентироваться в предложениях российских разработчиков, сформировать план последовательного перехода на российское ПО и „железо“ и способность его реализовать». Кроме того, дополнительным бонусом для IT-специалиста является наличие вендорского сертификата о прохождении курса по работе с программным продуктом. К специфическим требованиям для работы на объектах КИИ можно также отнести знание нормативов ФСТЭК и ФСБ, законодательной базы в сфере защиты информации, не составляющей государственную тайну, навыки ведения диалога с регуляторами, подготовки и ведения проектной документации, рассказал Виталий Терентьев.

Требования к специалистам в контексте КИИ больше относятся к умениям проходить аттестацию объектов и различные проверки, а специалистов с опытом в этой области «пока совсем мало», рассказывает Рустэм Хайретдинов. По его словам, в таком случае проще взять человека с техническими компетенциями и дотянуть его до умения взаимодействовать с регуляторами, чем искать готового специалиста. «Поэтому дополнительного спроса на IT-специалистов на объектах КИИ мы не наблюдаем»,— говорит господин Хайретдинов.

Но, в свою очередь, директор ДКИС ALP Group Светлана Гацакова утверждает, что на объектах КИИ дефицит аналитиков, разработчиков и экспертов в области информационной безопасности. Также, по ее словам, на рынке не хватает специалистов по комплексному управлению IT-проектами.

При этом HR-бренд объектов КИИ обычно проигрывает HR-брендам других частных компаний, и эту разницу работодатели закрывают зарплатами выше рынка, отмечает Артем Зыза. Зарплаты на этом рынке растут уже не первый год, но сильно зависят от конкретного предприятия КИИ и могут отличаться весьма существенно, говорит Светлана Гацакова.

Начинающий специалист с образованием и небольшим опытом или вообще без опыта работы может претендовать в регионах на 35–50 тыс. руб., в Москве — на 80–100 тыс. руб. в месяц с ежегодным ростом зарплаты, говорит Рустэм Хайретдинов. Продвинутый специалист с профильным опытом от трех-пяти лет может претендовать на 80–100 тыс. руб. в регионах и на 150–250 тыс. руб. в месяц в Москве. Квалифицированный специалист может претендовать на зарплату от 200 тыс. руб. в регионах и от 300 тыс. руб. в столице. Однако бывают и неруководящие IT-вакансии с предложениями на 800 тыс. руб. в месяц от российских компаний и на десятки тысяч долларов от американских и китайских организаций, добавляет господин Хайретдинов.

По данным hh.ru, средний уровень предлагаемых зарплат специалистам, взаимодействующим с КИИ, в России в 2021 году находится в пределах 65–155 тыс. руб. Зарплаты ведущим экспертам по информационной безопасности, консультантам, инженерам, главным специалистам по ИБ составляют 80–155 тыс. руб., рассказал Виталий Терентьев. С зарплатами от 200 тыс. руб. на hh.ru открыто немногим более сотни вакансий — такие зарплаты предлагают в основном директорам департаментов информационных технологий, экспертам, аналитикам, архитекторам информационной безопасности.

Юлия Степанова

Готовить кадры со школьной скамьи

— кадры —

Управляющий партнер ГК CommuniGate Systems АЛЕКСАНДР МАЛЫШЕВ о причинах кадрового дефицита в IT-отрасли и мерах борьбы с ним.

ПРЕДОСТАВЛЕНО ГК «COMMUNIGATE SYSTEMS»

За последние 10–15 лет появились сотни компаний, каждая из которых заинтересована набрать себе лучших IT-специалистов. В результате сегодня, по расчетам Минцифры, дефицит IT-кадров составляет от 500 тыс. до 1 млн человек и, по прогнозам, может увеличиться до 2 млн к 2027 году. Как же сложилось, что в сфере с практически самыми высокими зарплатами такой кадровый голод?

Сильная инженерная школа — МГУ, МГТУ имени Баумана и другие вузы — готовила талантливых программистов, которые обеспечили отечественному IT-рынку рывок в развитии. Сейчас эти кадры перешли на управляющие позиции, освободив рабочие места для поколения, которое получало образование уже во второй половине 1990-х и начале нулевых. Тогда приоритет в обучении сместился с точных наук на экономику, финансы, юриспруденцию. Дает о себе знать и демографическая яма 1990-х.

Кроме того, в IT-сфере появилось много новых направлений: интернет вещей, искусственный интеллект, виртуальная реальность, большие данные, мобильная разработка и многие другие. Если раньше софт ограничивался веб-версиями и десктопными вариантами, то теперь почти каждый продукт обязан быть представлен и в мобильной версии. Оклад опытного разработчика приложений превышает зарплаты топменеджмента отдельных компаний. IT-специалистов переманивают из регионов в столичные корпорации. Проработав в них несколько лет и повысив свой уровень, некоторые специалисты выходят на международный рынок труда, где их хантят уже зарубежные IT-гиганты. Это логичный процесс, поэтому необходимо заранее готовить смену.

Безусловно, заинтересованное в цифровизации страны и импортозамещении государство также видит проблему. Отрасли оказывается поддержка, реализуются программы по привлечению кадров в индустрию. Одна из стратегий — готовить их «со школьной скамьи». Крупные вендоры сотрудничают с вузами, стремясь выявить и «заполучить» наиболее талантливых студентов уже с первых курсов вузов.

CommuniGate Systems тоже всегда нужны высококвалифицированные мобильные разработчики. Мы пытаемся находить и обучать людей, а еще максимально разгружать разработчиков от выполнения побочных функций.

Что же делать IT-компаниям уже сейчас? Финансировать переквалификацию своих сотрудников под востребованные направления. Выделять отдельные направления разработки на аутсорсинг. Или можно обратиться к примерам из истории. Когда не хватало мощностей для постройки кирпичных домов, строители перешли к блочным технологиям, позволяющим упростить и ускорить процесс. Так и теперь — ситуацию, например, могут спасти low-code/no-code средства разработки, которые позволят создавать «блочное» ПО необходимого уровня из набора уже существующих инструментов специалистами даже с невысокой квалификацией.

Софт поставят по подписке

— инновации —

с13

«Кроме того, в системах CAD, PLM, ERP находятся данные, которые имеют не только коммерческую ценность, но и являются секретными. Вопрос легитимности работы с такими данными в условиях выхода информации за контур предприятия остается открытым»,— добавляет эксперт. Он отмечает, что разработчиков инженерного ПО в России единицы: «Их решения строились десятилетиями на собственных платформах и по собственной бизнес-логике. Такой же процесс происходит и в мире». Возможность объединения решений от разных вендоров в универсальном формате, по его мнению, злободневная, но пока не решенная задача. По данным IDC, суммарная выручка от продажи лицензий и поддержки корпоративного ПО в России по итогам 2020 года выросла на 6,7%, до 61,43 млрд руб.

Необходимость перемен

Предпосылки создания подобной единой платформы промышленного программного обеспечения были заложены в «дорожной карте» «Новые производственные технологии», которая была утверждена президиумом Правительственной комиссии по цифровому развитию в июле. Документ направлен на развитие программных решений для промышленности: технологий цифрового проектирования, математического моделирования, управления жизненным циклом продукции и «умного» производства. Картой предусмотрено также создание центров тестирования российского промышленного ПО. Ответственные за реализацию «дорожной карты» — государственные корпорации «Росатом» и «Ростех».

Предлагаемая к разработке платформа призвана обеспечить связь между разработчиками промышленного софта и предприятиями, отмечает директор по стратегическим проектам ГК «Цифра» Павел Федосов. «Иными словами, некий магазин приложений, где разработчики смогут выкладывать на платформу свои программные продукты, а предприятия, в свою очередь, смогут протестировать необходимые решения и впоследствии приобрети их по нескольким моделям, в том числе по подписке»,— объясняет он. Пока нигде в мире, по его словам, не было попыток внедрения подобных платформ на уровне государства. Сейчас во всем мире в части поставки промышленных IT-решений лидируют американские General Electric, PTC и европейские Siemens и Schneider Electric.

Порядок использования и подключения разработчиков и заказчиков к ММПП пока вызывает вопросы у участников рынка, отмечает Павел Федосов. В частности, есть риски, что унификация каналов доступа к заказчикам может привести к высоким комиссиям для разработчиков за продажу промышленного ПО — эта тенденция сейчас особо заметна в потребительских платформах прим. IOS, отмечает он. «Отдельный вопрос — как наполнить платформу и привлечь одновременно и заказчиков, и поставщиков, это вечная проблема всех маркетплейсов»,— добавляет эксперт. Но, по его словам, эти и другие вопросы сейчас активно прорабатываются с участниками рынка.

Главным преимуществом такой платформы для разработчиков может стать доступ к широкому рынку сбыта, считает Павел Федосов. «Плюсом могло бы быть и ускорение процессов принятия решений со стороны заказчиков. Дело в том, что специфика рынка промышленного ПО заключается в том, что одна сделка сейчас занимает от шести до девяти месяцев»,— объясняет он. Ускорить процедуру, по его словам, например, могла бы возможность заключать прямые контракты на основе быстрых конкурсов. Например, сейчас это реализовать практически очень сложно из-за необходимости соответствия 223-ФЗ. Для этого может быть использован механизм экспериментальных правовых режимов.

По мнению Павла Федосова, несмотря на масштабность, заложенную в саму суть ММПП, для эффективного запуска платформы необходимо обеспечить максимальное переиспользование уже готовых компонентов, наработок и решений игроков рынка, а также обеспечить бесшовную интеграцию с реестром отечественного ПО, порталом госзакупок и информационными системами Минпромторга России.

В целом, по мнению экспертов, создание универсальной платформы для промышленного ПО выглядит как логичный шаг на пути создания отечественных решений автоматизации и цифровизации промышленности в масштабах страны. В случае успеха инициатива, по их мнению, упростит включение разработчиков IT-решений в перечень поставщиков промышленных предприятий.

Юлия Тишина

Аппаратуру загрузят по-русски

— регулирование —

с13

Пилотный проект стартовал в МФЦ Орла, где установлены комплексные и полностью отечественные АРМ на базе компьютеров с российскими процессорами «Эльбрус8С» и Baikal-M (BE-M1000). В рамках проекта в МФЦ внедрили два АРМ — «Горыныч» и «ЭОС-Байкал». Предполагается, что применение обоих решений поможет госструктурам перейти на полностью отечественные сквозные решения, позволит оптимальнее расходовать средства и ускорит реализацию нацпроектов.

Другой значимый пример — представленный в июле в рамках конференции ЦИПР-2021 компанией TrueConf комплекс TrueConf 8 — пользовательское приложение со встроенным мессенджером и функциями видеоконференцсвязи (ВКС). Комплекс полностью совместим с российским ПК «Гравитон» на базе процессора Baikal-M и отечественной операционной системы Astra Linux. ВКС-приложение, по мнению разработчиков, призвано стать типовым отечественным решением для безопасной видеосвязи и корпоративного общения на рабочих местах.

Совместимость TrueConf 8 с российскими программными и аппаратными платформами позволит госкомпаниям обеспечить сотрудников безопасными продуктами для совместной работы и общения в соответствии с нормами кибербезопасности. Такой подход должен исключить риски недоступности ВКС и уязвимости, которые возникают при использовании зарубежных решений.

Вопрос совместимости российского ПО с «железом» возник одновременно со взятием курса на импортозамещение, напомнил заместитель гендиректора «РЕД СОФТ» Рустам Рустамов: «Заказчикам интересны исключительно ПАК, пригодные для реализации этой политики». Гармонизация реестра отечественного ПО с реестром оборудования, по его мнению, облегчит жизнь и заказчику, и разработчику. «Общая база позволит увидеть взаимно интегрируемые стеки. Плюс объединение реестров подтолкнет IT-компании к более активным действиям, направленным на подтверждение совместимости продуктов»,— полагает эксперт.

Очень важно создать полноценную российскую экосистему, включающую процессор, компьютер, операционную систему, прикладное ПО, подчеркивает Рустам Рустамов: «Операционная система „РЕД ОС“, например, уже совместима с широким спектром „железа“, в том числе на базе российского процессора „Байкал-М“. Российские прикладные решения прекрасно функционируют в среде „РЕД ОС“». Однако есть и обратная сторона медали, замечает эксперт: «Перенос сложного ПО будет дорогим, трудозатратным и длительным. К этому нужно быть готовым».

Дальнейшие шаги

Разработка и внедрение собственных программно-аппаратных платформ и комплексных решений необходимы для формирования технологической независимости России, отмечает исполнительный директор АРПП «Отечественный софт» Ренат Лашин: «Когда информационная инфраструктура организации построена на базе защищенных совместимых отечественных IT-решений, то и риск возможных санкций от иностранных производителей не будет угрожать стабильному функционированию ее систем, а шансы на удачную кибератаку, например, и утечку конфиденциальной информации или персональных данных значительно снижаются».

Внедрение отечественных IT-решений как в части программного обеспечения, так и в части аппаратного оборудования сейчас во многом стимулирует политика импортозамещения в этой сфере, проводимая на государственном уровне в последние годы, напоминает эксперт.

Разработчики отечественного софта уже давно сотрудничают с производителями оборудования — например, наиболее распространенные российские ОС работают практически со всеми отечественными процессорами, отмечает он.

Прикладное ПО, по мнению господина Лашина, также должно поддерживать аппаратную архитектуру отечественных процессоров, «ведь пользователю нужен не процессор и не ОС, а набор необходимых прикладных программ, реализующих заданный функционал». «Сегодня мы уже имеем значительный объем ПО, которое ни в чем не уступает своим иностранным конкурентам, а иногда даже превосходит — это и операционные системы, и офисные пакеты, средства электронного документооборота, защиты информации, виртуализации, криптографии, видеоконференцсвязи и другие»,— рассказывает эксперт. Уже, по его мнению, можно говорить о сформированной зрелой экосистеме отечественных решений, которые совместимы друг с другом и могут закрыть большинство запросов госсектора.

В свою очередь, АРПП «Отечественный софт», являясь крупнейшим отраслевым объединением разработчиков тиражируемого российского ПО, разработала и наполняет каталог его совместимости, говорит Ренат Лашин: «Это позволяет госсектору не только подбирать совместимое российское ПО, но и использовать сведения о решениях при разработке и последующей цифровой трансформации». Кроме этого, добавляет эксперт, при активном участии Ассоциации в настоящее время проводится работа по созданию критериев для синхронизации реестра отечественного ПО Минцифры и реестра оборудования Минпромторга и последующему внесению в них сведений о совместимости отечественного ПО с оборудованием.

Юлия Тишина

Review Российский софт для значимой инфраструктуры

ЦРТ ГРУППА КОМПАНИЙ МойОфис

Цифра сложилась с госсектором

Начиная с прошлого года все ключевые отрасли экономики, социальной сферы, министерства и ведомства озаботились необходимостью цифровой трансформации во исполнение поручения президента. В ближайшие годы для повышения эффективности работы и взаимодействия с гражданами в госсекторе необходимо будет внедрить и адаптировать к специфике деятельности технологии искусственного интеллекта, большие данные, интернет вещей, голосовые ассистенты и многие другие IT-решения. Такая инициатива призвана в ближайшей перспективе поддержать рост отечественных разработчиков, решения которых уже сейчас способны, по экспертным оценкам, закрыть до 90% всех потребностей органов власти и бизнеса.

— тренды —

АНАТОЛИЙ ЖДАНОВ

Цифровую трансформацию в качестве национальной идеи развития до 2023 года президент Владимир Путин определил еще в прошлом году. За ближайшие десять лет «цифровой зрелости» должны достичь ключевые отрасли экономики и социальной сферы, в том числе здравоохранение и образование, а также государственное управление. Доля массовых социально значимых услуг, доступных в электронном виде, должна составить 95%, доступ к высокоскоростному интернету — получить до 97% домохозяйств, а инвестиции в отечественные разработки в области информационных технологий — увеличиться в четыре раза по сравнению с 2019 годом.

В числе наиболее востребованных IT-направлений, на внедрение которых ведомства должны бросить свои усилия, — искусственный интеллект, большие данные и интернет вещей, а также российская радиоэлектронная продукция: системы хранения данных, серверное оборудование, камеры видеонаблюдения и другое оборудование. Также ведомства должны перейти на использование ГосОблака Минцифры. В эксперименте по переходу уже принимают участие более 20 ведомств. По результатам эксперимента проект будет масштабирован на все органы власти. ГосОблако выполняет роль инфраструктурного фундамента, который предоставляет вычислительные ресурсы, обеспечивает безопасность данных, в том числе благодаря использованию преимущественно российского программного обеспечения и оборудования.

За счет использования облачной платформы ведомства экономят на обслуживании собственной IT-инфраструктуры. «Активная цифровизация госорганов сопровождается увеличением количества запросов, регистрируемых в Госинформсистеме координации информатизации (ФГИС КИ). В системе происходит согласование закупок, которые поддерживают деятельность ведомств, следовательно, сбои в ее работе недопустимы. Нам удалось реализовать бесшовный переход на облачную платформу и обеспечить непрерывное функционирование системы»,— отмечали ранее в Минцифры.

С точки зрения государства задача стоит в повышении эффективности и создании добавленной стоимости во всех отраслях экономики за счет системного внедрения цифровых технологий, отмечает партнер практики технологического консалтинга PwC в России Тимофей Хорошев. При этом, отмечает он, ставится задача реализации суверенной цифровой трансформации. «А это значит, что роль отечественных разработчиков в этом процессе трудно переоценить. И если сегодня предприятия все еще могут делать выбор в пользу возможно более развитых и более функциональных зарубежных решений, тем не менее со временем предприятия будут двигаться в сторону локализации подобных систем»,— подчеркивает эксперт.

Эффективность под прицелом

Цифровизация предполагает использование современного пула технологий, не последнее место в которых занимает внедрение отечественного ПО, отмечает коммерческий директор ГК CommuniGate Systems Владимир Бургов. При поддержке правительства российские разработчики активно развивают свои продукты, расширяют линейки решений, становятся центром компетенции по разработке софта для цифровой трансформации, отмечает он.

По предварительным оценкам, решения, которые сейчас входят в Единый реестр отечественного ПО, закрывают порядка 90% запросов органов власти и бизнеса, говорит эксперт. «Это приносит свои результаты — например, в 2020 году вдвое (с 25% до 48%) выросло число госкомпаний, осуществляющих цифровую стратегию. Мы наблюдаем рост использования голосовых помощников и интеллектуальных чатботов, использование ИИ при обработке массивов информации»,— рассказывает Владимир Бургов. Однако вендору уже недостаточно просто создать новый продукт, отмечает он. «Разработчик должен учитывать последующее обучение госслужащих работе с этим ПО, чтобы они смогли полноценно использовать новые методы работы. Цифровая трансформация не будет реализована, если конечный пользователь не будет знать, как использовать ее инструменты в своей работе»,— подчеркивает он.

Массовое обслуживание в чате и голосовых каналах сегодня является одним из самых быстро растущих направлений в области цифровизации госсектора. Так, согласно исследованию Gartner Digital Transformation Divergence Across Government Sectors, чат-боты и диалоговые системы лидируют по внедрению в госсекторе во всем мире, где около 26% респондентов сообщили, что уже применяют такие ИИ-технологии, а еще 59% опрошенных намерены сделать это в ближайшие три года. Gartner оценивает уровень проникновения текстовых роботов в бизнесе сегодня в 50%, а также считает, что к концу 2021 года уже 25% компаний по всему миру будут иметь виртуального помощника для решения вопросов поддержки.

Сотни информационных систем государства в рамках программы цифровизации федеральных органов исполнительной власти требуют перехода от автоматизации конкретных функций к клиентоцентричному подходу, отмечает гендиректор группы компаний ЦРТ Дмитрий Дырмовский: «Важный элемент стратегии — применение ИИ-решений в тех областях, где возникает потребность в автоматизации взаимодействия с населением,— это различные массовые сервисы госсектора». По его мнению, наиболее перспективными в этой части станут масштабируемые сервисы, которые не требуют длительного времени на построение, легко внедряются между регионами. Так, по его словам, хороший пример — Госсервис 122: каждый отдельный регион может получать готовый сервис на базе облака, не вдаваясь в подробности технической реализации.

Так ИИ позволяет обеспечить бесшовное и быстрое подключение регионально важного сервиса за минимальный срок. Наряду с готовой реализацией виртуального оператора технологии ИИ в области анализа и распознавания речи в ближайшее время получат еще большее развитие, уверен Дмитрий Дырмовский. Успешный опыт цифровизации демонстрирует крупный бизнес: 27 из крупнейших 50 банков и топ-5 телеком-компаний России, по словам эксперта, используют ИИ-решения компании: наиболее востребованы речевая аналитика, текстовые и голосовые роботы. «Доказавшие эффективность решения могут помочь и в госсекторе. За последние три года группа ЦРТ реализовала более 280 проектов по цифровизации государственных и муниципальных учреждений в 85 субъектах страны»,— добавил Дмитрий Дырмовский.

Отечественные возможности

Отечественные разработчики присутствуют в большинстве направлений, традиционно связываемых с цифровой трансформацией. В их числе, по словам Тимофея Хорошева, большие данные и продвинутая аналитика, искусственный интеллект, технологии дополненной и виртуальной реальности, беспилотные транспортные средства, облачные технологии, мобильные технологии, класс традиционных продуктов в области автоматизации бизнес-процессов предприятия. В этих и многих других направлениях успешно ведутся отечественные разработки, выводятся на рынок новые конкурентные продукты, отмечает эксперт.

Если говорить об экспортном потенциале, речь идет прежде всего о возможности продвижения своих позиций на рынках третьих стран, отмечает Тимофей Хорошев. «Там, где еще не заняты соответствующие ниши и при этом нет достаточных ресурсов для разработки собственных цифровых технологий. Таким игрокам российские поставщики, по сути, предлагают альтернативу западным технологиям и делают этот рынок более конкурентным в глазах покупателя»,— объясняет он.

Партнер консалтинговой компании Bright Александр Ракша утверждает, что в последние годы отмечается постепенный качественный рост российских разработчиков, которые создают цифровые и IT-решения для крупных заказчиков. «Пока все эти решения в сложных индустриях ограничены правилами закупок и фрагментированностью рынка, поэтому разработка сопряжена с большими издержками на адаптацию и внедрение под конкретного заказчика»,— рассказывает он. Но при условии снятия этих ограничений доля российских вендоров может существенно вырасти в ближайшие три-пять лет, допускает эксперт.

По его мнению, российские вендоры уже становятся центром компетенции по разработке ПО для цифровой трансформации. «Более того, появляются уже знаковые проекты в сегментах платформенных решений для цифровой трансформации, которые сопоставимы с зарубежными аналогами, а в некоторых сегментах решений Индустрии 4.0 уже конкурируют на мировом рынке»,— отмечает Александр Ракша. Мы уже сейчас видим огромный рост в таких перспективных нишах, как low-code и no-code решениях, в промышленном интернете вещей, а российские решения для финтеха являются одними из наиболее развитых в мире, подчеркивает он.

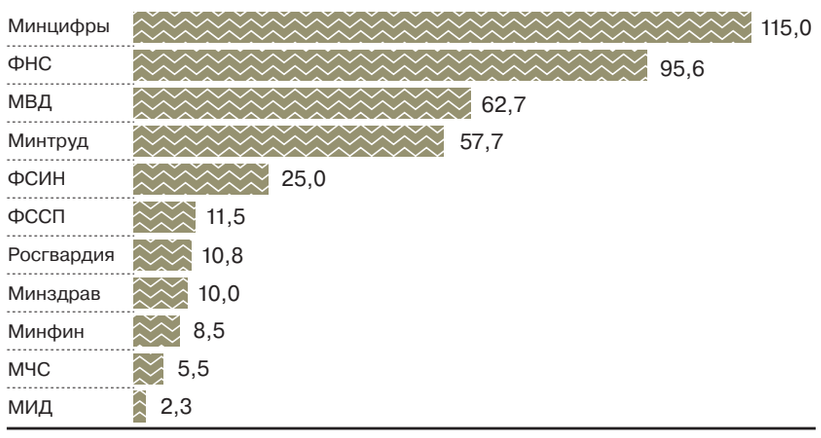
Гендиректор АНО «Цифровые платформы» Арсений Щельцин убежден, что отечественные разработчики уже являются не только центрами компетенций в части цифровой трансформации госсектора, но и экономической и социальной сферы. «В плане программного обеспечения, я считаю, у нас все хорошо. До оценки „отлично“ не хватает массового внедрения отечественных продуктов и большой вовлеченности разработчиков в бизнес-задачи. Нам достаточно продуктов для себя и для экспорта в сфере информационной безопасности: от криптографических инструментов до локальных утилит оценки трафика и уязвимостей»,— рассуждает эксперт. По его мнению, успешными также являются офисные приложения: от минимального пакета визуальных редакторов до систем 3D-моделирования, управления компанией и деловыми процессами. «Достойное программное обеспечение в сфере управления ресурсами предприятий, управление производством, однако также есть много пробелов в плане адаптивности. Превосходные продукты в сфере управления контентом — от систем управления сайтом до систем мониторинга и систем аналитики больших данных»,— отмечает Арсений Щельцин.

Если говорить о новых направлениях, у нас одни из лучших команд по искусственному интеллекту, блокчейну, огромное количество разработчиков делают VR&AR-приложения, говорит эксперт. «Хорошие наработки и большая экспертная энергия также в сфере квантовых технологий. В планах множество других параллельных движений, таких как развитие open source сообщества, собственные средства производства и компиляторы и др. При естественном ходе вещей России удастся добиться успеха»,— убежден он.

Однако руководитель технологической практики КПМГ в России и СНГ Николай Легкодимов отмечает, что в контексте цифровизации госсектора на российском IT-рынке сложилась парадоксальная ситуация: «Своими IT-подразделениями обзавелись практически все крупные государственные и окологосударственные игроки, что привело не только к разгону зарплатных ожиданий IT-специалистов, но и к перераспределению традиционных ролей между участниками рынка». Таким образом, традиционная модель IT-вендора с одной стороны, консультантов — с другой, потребителей проекта — с третьей, а регулятора — с четвертой пополнилась пятой ролью, которая начинает играть все большее значение,— кэптивных IT-компаний крупных банков, нефтяных, телекоммуникационных и других участников рынка. Эта последняя категория в силу практически неограниченного ресурса и отсутствия жестких требований к эффективности проектов, скорее всего, и станет одним из основных агентов проведения цифровой трансформации на уровне страны, предполагает эксперт.

Юлия Тишина

ЗАТРАТЫ КЛЮЧЕВЫХ ВЕДОМСТВ НА ЦИФРОВУЮ ТРАНСФОРМАЦИЮ ДО 2023 ГОДА (МЛРД РУБ.) ИСТОЧНИК: ПОРТАЛ ФГИС КИ.



Нейросети идут на помощь

— инновации —


ПРЕДОСТАВЛЕНО «ЦРТ»

Гендиректор группы ЦРТ ДМИТРИЙ ДЫРМОВСКИЙ о том, как искусственный интеллект помогает лучше понимать потребности граждан.

Сегодня ключевая цель цифровизации для бизнеса — удовлетворение потребностей клиента, а для государства — потребностей граждан, создание экосистемы городских сервисов. Такие цели формируют клиентоцентричный подход. При этом современные технологии могут улучшить коммуникации с жителями, помогают «лучше слышать и понимать» их для более эффективного управления городскими сервисами.

В целом потребность «слышать голос» потребителей и на основе этого совершенствовать сервисы, создавать новые услуги уже стала стандартом. Крупный бизнес, банки, телеком-операторы, e-commerce давно успешно используют искусственный интеллект (ИИ) для оптимизации дистанционного взаимодействия: выявляют наиболее частые запросы, внедряют речевую аналитику. По оценке Gartner, именно чат-боты в настоящее время являются наиболее частым вариантом применения ИИ в бизнесе.

Эффективный опыт бизнеса в области внедрения искусственного интеллекта, в том числе автоматизация обслуживания с помощью качественных текстовых и голосовых роботов, может быть масштабирован и на взаимодействие с государством. К примеру, с помощью ИИ-решений можно обрабатывать обращения в МФЦ или запись к врачу.

Так, с помощью сервиса голосового ввода медицинских документов Voice2Med, разработанного ЦРТ, врачи-рентгенологи Москвы подготовили более 95 тыс. протоколов. Это решение работает уже в 30 регионах России. Группа ЦРТ также разработала робота-оператора, который может обзванивать пациентов, напоминать о предстоящем визите к врачу, сообщить, как подготовиться к процедурам. В случае отказа от записи виртуальный ассистент может отменить прием и предложить другое время. Только за первые три недели работы виртуальный ассистент помог четверти пациентам «УГМК-Здоровье» в Екатеринбурге отменить прием или скорректировать дату и время визита, а на свободное место записать новых пациентов, что снизило финансовые потери клиники. Другой пример — чат-бот «Мосметро» «Александра» (разработан ЦРТ совместно с «Московским метрополитеном») уже обрабатывает 88% запросов без перевода на оператора.

Локдаун показал, насколько важна связь со своей целевой аудиторией, в том числе в дистанционных каналах. Сегодня есть ряд уже готовых решений, которые могут поддержать развитие городских сервисов на необходимом технологическом уровне. Но важно выбирать проверенные решения: качественный, реалистичный синтез речи робота, «интеллект», позволяющий реагировать на перебивания, опыт реальной интеграции в инфраструктуру. В противном случае такие внедрения могут привести лишь к проблемам и раздражению пользователей.

Зачем обеспечивать информационную безопасность офисного ПО?

— безопасность —


ПРЕДОСТАВЛЕНО «МОЙОФИС»

ДМИТРИЙ КОМИССАРОВ, гендиректор компании— разработчика «МойОфис», о стратегии сокращения рисков на объектах критической информационной инфраструктуры (КИИ).

Важность перевода объектов КИИ на российское программное обеспечение обоснована двумя факторами: санкционными рисками, которые ограничивают возможности по использованию иностранного ПО, и резким увеличением числа инцидентов информационной безопасности (ИБ). С рисками первой категории уже сталкивались российские предприятия и учебные заведения — так, в 2019 году «Газпрому» принудительно отключили импортную технику через спутник, а «Росатому» и МГТУ имени Баумана отказались продавать лицензии на программное обеспечение.

Опасность представляют и риски в области ИБ. За неполный 2021 год в России уже зафиксировано почти в три раза больше атак на объекты критической инфраструктуры, чем за весь 2019 год. Только в 2020 году центр мониторинга и реагирования на кибератаки Solar JSOC обнаружил 200 атак профессиональных кибергруппировок.

В этой связи поставщики ПО для объектов КИИ должны создавать безопасные продукты и гарантировать независимость от геополитических условий и санкционных рисков. Подтверждением этому может считаться только наличие лицензий и сертификатов, которые выдают регуляторы. Для повышения безопасности информационных систем на объектах КИИ разработчики системного и прикладного ПО строят модели угроз для своего ПО, анализируют архитектуру продукта и проверяют исходный код тестированием на проникновение. Сертификация также обеспечивает проверку исходного кода на отсутствие недекларированных возможностей.

КИИ — сложная система, которая включает не только средства защиты, но и прикладное ПО. Так, по данным «Лаборатории Касперского», акционера «МойОфис», более 70% угроз безопасности вызваны уязвимостями именно в офисном ПО. Поэтому использование безопасных версий такого софта является необходимым требованием для защиты данных на объектах КИИ.

Сегодня «МойОфис» является единственным российским офисным решением, безопасность которого подтверждена ФСТЭК России, ФСБ и Минобороны. Более того, в России только нашим облачным продуктам удалось успешно пройти комплекс испытаний во ФСТЭК России и получить сертификат на все облако целиком, а не только на его отдельные части. При разработке приложений «МойОфис» уделяет большое внимание вопросам безопасности, которые заложены на уровне архитектуры продуктов. Это гарантирует контроль над данными пользователей и высокую защиту от утечек информации.

Приложение к газете «Коммерсантъ» (Review «Российский софт для значимой инфраструктуры»). | Владимир Желонкин — генеральный директор АО «Коммерсантъ», главный редактор | Сергей Вишневский — руководитель фотослужбы | Рекламная служба: Тел. (495) 797-6996, (495) 926-5262 | Владимир Лавицкий — директор «Издательского синдиката» | Юлия Тишина — выпускающий редактор | Ольга Еременко — редактор | Сергей Цомык — главный художник | Галина Кожеурова, Екатерина Репях — фоторедакторы | Екатерина Бородулина — корректор | Ограничение: 16+