

САНКТ-ПЕТЕРБУРГ ЦИФРОВАЯ ЭКОНОМИКА

НОВАЯ ФОРМА
ДЛЯ НАЦВАЛЮТЫ / 3
КОНСУЛЬТАЦИЯ
НА РАССТОЯНИИ / 4
КОМПАНИИ МЕНЯЮТ
КИБЕРЩИТ / 6

Вторник, 31 октября 2023
Тематическое приложение
к газете «Коммерсантъ» №31

Коммерсантъ
ONLINE

BUSINESS GUIDE

Коммерсантъ

В лучших местах Петербурга

РЕСТОРАНЫ

«Кремль»	Выборгская наб., 55 (БЦ Gregory's Palace)
Ресторан-гостиница «Штакеншнейдер»	Миллионная ул., 10
«Шляпин»	Тверская ул., 12/15
Таверна «Гролле»	Большой пр. В. О., 20
«Сказка Востока 1001 ночь»	Лесной пр., 48
Stroganoff Steak House	Конногвардейский б-р, 4
«Метаморфоз»	Литейный пр., 5/19
Ресторан русской кухни Siberika	Лейтенанта Шмидта наб., 43
Cafe Claret	Марата ул., 11
Marius	Марата ул., 11
Ресторан Частного клуба «Профессор Фрейд»	Малая Морская ул., 18
SETTLERS	Наличная ул., 24/1 А
«АЛКОБУФЕТ ПЕЛЬМЕННАЯ»	Б. Конюшенная ул., 29
Бар-ресторан «География»	Рубинштейна ул., 5
Ирис	Декабристов ул., 57
Ресторан Parfait	Парфеновская ул., 9, к. 2 (вход с Измайловского б-ра)
Ресторан MEZE	Московский пр., 206
Ресторан Cast	Каменноостровский пр., 10 А
Гастробар «Чайки»	Мошков пер., 5 Б

КАФЕ

Kroo cafe	Суворовский пр., 27 / 9-я Советская ул., 11
Кафе «Моцарт»	Кронверкский пр., 23
Пространство Freedom	Казанская ул., 7

ГОСТИНИЦЫ

Отель «Индиго»	Чайковского ул., 17
Akuan Hotel	Восстания ул., 19
M-hotel	Садовая ул., 22 (вход с переулка Крылова, 2, со двора)
«Гранд Отель Эмеральд»	Суворовский пр., 18
Majestic Boutique Hotel Deluxe	Садовая ул., 22/2
The Gamma Hotel	наб. Обводного кан., 130
Grani Aparthotel	Большая Зеленина ул., 24
Trezzini Palace Hotel	Университетская наб., 21
Welton Club Hotel & Apartments	Малая Разночинная ул., 11
Four Seasons Hotel	
Lion Palace St. Petersburg	Вознесенский пр., 1
Crowne Plaza St. Petersburg — Ligovsky	Лиговский пр., 61
Официальная гостиница «Эрмитаж»	Правды ул., 10
Author Boutique Hotel	Владимирский пр., 9
Airportcity Plaza St. Petersburg	Стартовая ул., 6 А
«Гранд Отель Мойка 22»	наб. реки Мойки, 22
«А1 Отель Санкт-Петербург»	Кирпичный пер., 3

«Cronwell Inn Стремянная»	Стремянная ул., 18 А
Бутик-отель «Северный цветок»	Марата ул., 40
Отель «Братья Карамазовы»	Социалистическая ул., 11 АВ
Отель «Гельвеция»	Марата ул., 11
MoLo	Вс. Вишневого ул., 2/12 К
Екатерина	Миллионная ул., 10
Отель «Мартин»	Марата ул., 12
Sokroma Boho	Средняя Подъяческая ул., 4 А
«Лотте Отель Санкт-Петербург»	пер. Антоненко, 2, стр. 1
Отель «Невский Берег»	Невский пр., 122

ИНТЕРЬЕРНЫЕ МАГАЗИНЫ

Салон «Сентябрь»	Каменноостровский пр., 19
------------------	---------------------------

ЧАСОВЫЕ И ЮВЕЛИРНЫЕ МАГАЗИНЫ

Мультибрендовый бутик Spblux	Большая Конюшенная ул., 17
------------------------------	----------------------------

БИЗНЕС-ЦЕНТРЫ

Gregory's Palace	Выборгская наб., 55
Gustaf	Средний пр. В. О., 36/40
Деловой центр NEVKA	Гельсингфорсская ул., 3, к. 11 Д, вход с Выборгской наб., 45-47
Magnus	9-я линия В. О., 34
«Оскар»	наб. р. Фонтанки, 13 А
Коворкинг «Пушкин»	Торжковская ул., 5

АВТОСАЛОНЫ

Автодом «Пулково»	Пулковское ш., 14 А
Gregory's Cars	Выборгская наб., 55
Петровский на Софийской	Софийская ул., 87

АВИАКОМПАНИИ

ЦБА «Пулково-3»	
ГТК «Россия»	

РАЗНОЕ

Миграционный центр	Красного Текстильщика ул., 10/12
Поезда «Сапсан»	бизнес-класс
Аэропорт Пулково	бизнес-залы, VIP-зал



Узнайте подробную информацию о корпоративной подписке по телефону **8 800 600 0556** (звонок по России бесплатный) или электронной почте podpiska@kommersant.ru

www.kommersant.ru



ВАЛЕРИЙ ГРИБАНОВ,
РЕДАКТОР BUSINESS GUIDE
«ЦИФРОВАЯ ЭКОНОМИКА»

СЪЕХАТЬ С НАКАТАННОЙ ТРАЕКТОРИИ

Цифровизация в России продолжает активное развитие, несмотря на серьезные сложности, вызванные санкциями. Даже для многих технологически развитых стран привычки жителей крупных городов России выглядят несколько диковинно: в части взаимодействия с бюрократическими структурами и финансовыми учреждениями российский цифровой опыт в некотором смысле оказался передовым. Впрочем, далеко не во всем: развитие телемедицины, например, серьезно отстает от той же Америки, хотя в условиях огромных расстояний и плохих дорог как раз именно это направление было бы логично развивать одним из первых.

Последние полтора года все силы отечественных сотрудников высокотехнологичной сферы брошены на уход от западных продуктов и полного обособления IT-сферы. Вероятно, это несколько затормозит прикладную цифровизацию различных сфер российской жизни. С другой стороны, то, что перед разработчиками поставлена амбициозная задача поиска принципиально новых решений, вероятнее всего, приведет к сопутствующим открытиям и внедрениям.

Тут уместна аналогия с военно-промышленным комплексом: инвестиции в него рождают попутные открытия, полезные и в гражданской сфере. Так же и с IT-сектором: вложения в системы безопасности, создание собственных платформ, уход от накатанной дороги предоставят возможность создавать продукты, которые имеют шанс стать передовыми и прорывными.

НОВАЯ ФОРМА ДЛЯ НАЦВАЛЮТЫ

В АВГУСТЕ ПОСЛЕ ВСТУПЛЕНИЯ В СИЛУ СООТВЕТСТВУЮЩЕГО ЗАКОНА В РОССИИ НАЧАЛОСЬ ПИЛОТИРОВАНИЕ ЦИФРОВОГО РУБЛЯ. ЭКСПЕРТЫ РАССКАЗАЛИ О ВОЗМОЖНОСТЯХ И РИСКАХ, КОТОРЫЕ НОВАЯ ФОРМА НАЦИОНАЛЬНОЙ ВАЛЮТЫ НЕСЕТ СВОИМ ПОЛЬЗОВАТЕЛЯМ. АНТОНИНА ЕГОРОВА

Цифровой рубль является новой формой рубля — наравне с существующими сейчас наличной и безналичной. Однако существенных отличий при его использовании для отдельно взятого гражданина или коммерческой организации, по словам экспертов, будет немного.

Как отмечает Евгений Калянов, эксперт по фондовому рынку «БКС Мир инвестиций», основное его отличие от безналичной формы в том, что цифровая национальная денежная единица применяет технологию блокчейна. Новая форма рубля представляет собой уникальный цифровой код. Единственным оператором платформы цифрового рубля будет Центробанк. В отличие от криптовалюты, у цифрового рубля есть централизованный эмитент, несущий ответственность за валюту: Банк России. При этом если безналичные денежные средства отражаются на счете, открытом в любой банковской организации, цифровой рубль будет учитываться на электронном кошельке, открытом на платформе Центрального Банка. Коммерческие банки в этом случае будут являться лишь посредниками, осуществляющими открытие кошельков и предоставляющими к ним доступ, в том числе через свои приложения.

Каждый россиянин сможет открыть цифровой кошелек, но только один. Лимит его пополнения составит 300 тыс. рублей в месяц. Расчеты в цифровых рублях будут быстрее, чем в безналичной форме. Как отмечает Евгений Безручкин, помощник юриста ООО «Мариокс центр», цифровыми рублями можно будет расплачиваться даже без подключения к интернету.

«Переводы в новой форме валюты будут бесплатными. Также сумма бесплатных переводов будет как минимум в три раза выше, чем в системе быстрых платежей. Ставка комиссии для юридических лиц будет установлена в районе 0,3%, что существенно ниже действующих банковских процентов. При этом новая форма национальной валюты предусмотрена только для переводов и платежей, но не для сбережений. Кредитов и кешбэка в цифровых рублях не будет», — сообщает господин Калянов.

Как поясняет Елена Козина, старший партнер адвокатского бюро «ЭЛКО профи», конвертация цифрового рубля в наличные и безналичные средства осуществляется в соотношении 1:1. Однако если перевести цифровой рубль в средства на банковском счету можно мгновенно, то перевод наличных рублей в цифровые и наоборот пока может происходить только через перевод в безналичную форму с использованием банковского счета.

ВОЗМОЖНОСТИ И РИСКИ В первую очередь, по словам Алексея Балашова, заместителя председателя комитета по финансовым рынкам Санкт-Петербургской торгово-промышленной палаты, возможности новой формы национальной валюты видятся в тонких настройках платежей, которые позволят контролировать целевое использование эмитированных средств, а также в экономии издержек на сами транзакции и в том, что Банк России как оператор платформы сможет гарантировать сохранность средств, так как деньги будут находиться не в банке, у которого могут отозвать лицензию.

Существенным плюсом распространения платежей посредством цифровых рублей, по словам госпожи Козиной, является потенциальная возможность преодоления

санкций и осуществления расчетов с иностранными контрагентами, так как осуществлять переводы будет возможно без участия SWIFT — с помощью другой системы, разработка которой сейчас ведется.

«Для государства введение новой формы рубля имеет более существенное значение, чем для конкретного гражданина. С учетом того, что цифровой рубль является платежным средством в виде цифрового кода, эмитентом которого является Центробанк, все операции с его применением находятся под контролем государства. Осуществление платежей с помощью новой формы рубля делает транзакции прозрачными, которые в контексте государственного регулирования рассматриваются как безопасные», — указывает эксперт.

По словам Олега Анисимова, основателя проекта «Вклады», цифровой рубль позволит государству более технологично решать некоторые задачи. Например, ограничивать, на что будет потрачен конкретный рубль. Это упростит бюджетную бюрократию. «Допустим, человек получает грант, который можно потратить только на частичную оплату обучения в российских вузах, или детские пособия на определенные цели, или субсидии. Хотя по аналогии с наличными каждый цифровой рубль имеет условный номер, как и бумажная купюра, в бумажном обращении по номеру купюры все равно ничего не отследишь, а тут будет реестр, в котором все транзакции этого рубля — от выпуска до последнего держателя — будут зафиксированы. Соответственно, контрагентов по цифровому рублю лучше выбирать внимательнее, чтобы не стать соучастником противозаконного деяния», — поясняет он.

К другим особенностям использования цифровой формы рубля можно отнести упрощение порядка взыскания данных средств по исполнительным документам. В данной концепции, по словам экспертов, взыскание денежных средств в цифровой форме может осуществляться, если имеется недостаток наличных или безналичных средств. Однако с учетом того, что электронный кошелек будет открыт на платформе Центробанка, у взыскателя отпадает необходимость поиска счетов в существенном массиве банковских организаций. В целом больший контроль со стороны государства не сможет уберечь цифровой рубль от рисков, которые в первую очередь связаны с его цифровой формой.

«С учетом того, что доступ к кошельку будет осуществляться через приложение с использованием стандартных ключей-паролей, так же, как и при использовании безналичных денежных средств, остается риск несанкционированного доступа к ним и последующего вывода с использованием вредоносного программного обеспечения», — обращает внимание госпожа Козина.

ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ Теоретически, по мнению Дмитрия Панова, председателя петербургского отделения «Деловой России», цифровой рубль может быть использован во всех транзакциях, однако на практике могут возникнуть сложности. Во-первых, пополнить цифровой кошелек возможно только списанием с банковского счета, аналогичным образом можно будет вывести электронные рубли. Во-вторых, для оплаты товаров или услуг потребуются мобильное приложение и считывание QR-кода, что может быть затруднительно для пожилых людей и отдельных социально незащищенных категорий граждан. Кроме этого,

пока что открытыми остаются вопросы безопасности и защиты цифровых рублей от мошенничества.

«В тестировании использования новой формы рубля, которое началось в августе, участвуют несколько крупных российских банков. В результате этой апробации перед разработчиками системы будет стоять необходимость оттачивания механизмов открытия, закрытия и обслуживания кошельков, на которых будет происходить учет цифрового рубля, а также осуществления операций по конвертации цифровой валюты в давно привычные формы, осуществление платежей и расчетов. По итогу прохождения тестового периода можно будет сделать конкретные выводы о готовности программного обеспечения или необходимости создания дополнительной инфраструктуры для комфортного использования рубля в цифровой форме», — говорит госпожа Козина.

Как отмечает господин Балашов, на первом этапе Банк России планировал выплачивать заработную плату своим сотрудникам цифровыми рублями для проведения эксперимента и дальнейшего тиражирования платежей, а также использовать как источник маркированных денег, например, для оплаты субсидиями на ЖКХ только платежей в пользу ЖКХ.

«Несмотря на многочисленные вопросы к цифровому рублю и механизму его использования, есть все основания полагать, что перспективы у него довольно серьезные. Подтверждением этому можно считать намерение одного из экспертов петербургской «Деловой России» — компании «Теремок» — принять участие в пилотном эксперименте Центробанка по использованию цифрового рубля в расчетах за свою продукцию, в связи с чем уже направлено официальное обращение в адрес Банка России», — отмечает господин Панов.

«Введение цифрового рубля в контексте конкретного потребителя не будет являться чем-то особенным, так как формат его использования будет сильно похож на использование уже привычных всем безналичных денежных средств. Потенциальная возможность осуществления трансграничных платежей без использования системы SWIFT является серьезным фактором, который добавляет интереса к новой форме рубля со стороны юридических лиц», — считает Елена Козина. Распространение платежей с использованием цифрового рубля среди юрлиц планируется на 2024 год, а введение его во всеобщее использование — ориентировочно на 2025 год. ■

СУЩЕСТВЕННЫМ ПЛЮСОМ РАСПРОСТРАНЕНИЯ ПЛАТЕЖЕЙ ПОСРЕДСТВОМ ЦИФРОВЫХ РУБЛЕЙ ЯВЛЯЕТСЯ ПОТЕНЦИАЛЬНАЯ ВОЗМОЖНОСТЬ ПРЕОДОЛЕНИЯ САНКЦИЙ И ОСУЩЕСТВЛЕНИЯ РАСЧЕТОВ С ИНОСТРАННЫМИ КОНТРАГЕНТАМИ, ТАК КАК ОСУЩЕСТВЛЯТЬ ПЕРЕВОДЫ БУДЕТ ВОЗМОЖНО БЕЗ УЧАСТИЯ SWIFT — С ПОМОЩЬЮ ДРУГОЙ СИСТЕМЫ, РАЗРАБОТКА КОТОРОЙ СЕЙЧАС ВЕДЕТСЯ



КОНСУЛЬТАЦИЯ НА РАССТОЯНИИ

ТЕЛЕМЕДИЦИНА, ИЛИ ДИСТАНЦИОННОЕ ПРЕДОСТАВЛЕНИЕ МЕДИЦИНСКИХ УСЛУГ,— В РОССИИ ОТНОСИТЕЛЬНО НОВОЕ НАПРАВЛЕНИЕ, АКТИВНОЕ РАЗВИТИЕ КОТОРОГО ПРИШЛОСЬ НА ПЕРИОД ПАНДЕМИИ. И ХОТЯ С УЧЕТОМ ОГРОМНЫХ РАССТОЯНИЙ В СТРАНЕ ЭТОТ ВИД ВЗАИМОДЕЙСТВИЯ ВРАЧЕЙ С ПАЦИЕНТАМИ И КОЛЛЕГАМИ ИМЕЕТ ВСЕ ШАНСЫ БЫТЬ КРАЙНЕ ВОСТРЕБОВАННЫМ, ЕГО ВНЕДРЕНИЕ ПОКА ИДЕТ НЕВЫСОКИМИ ТЕМПАМИ.

АНТОНИНА ЕГОРОВА

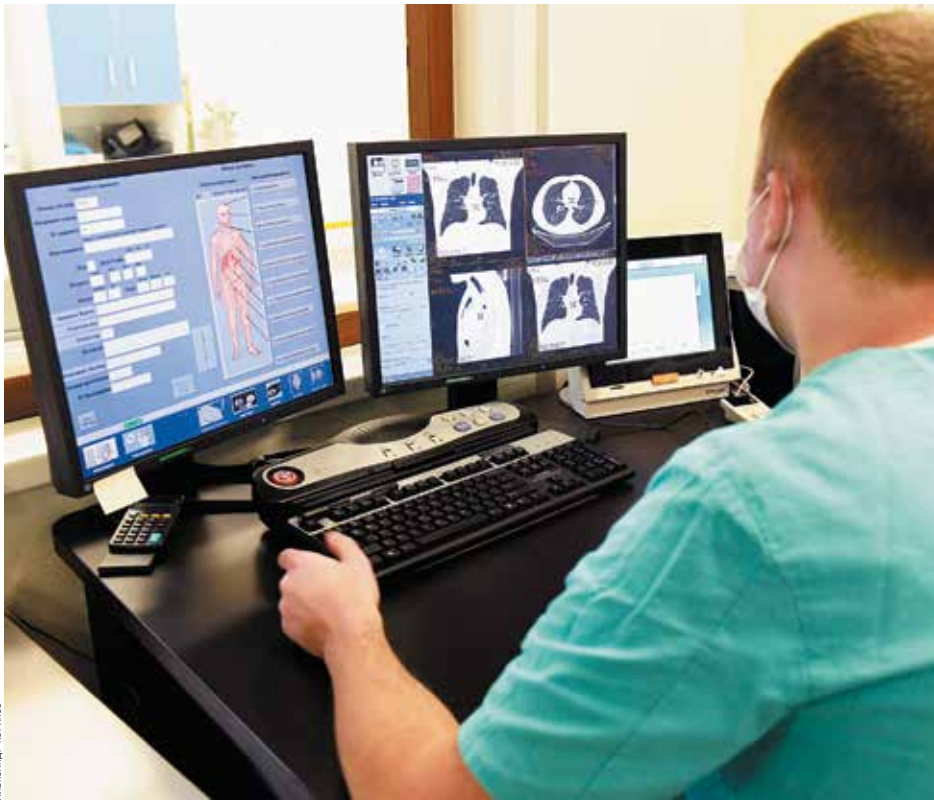
Понятие «телемедицина» введено федеральным законом 323-ФЗ, вступившим в силу с 1 января 2018 года, порядок оказания телемедицинских консультаций также регулируется ведомственными приказами Минздрава. Телемедицина подразумевает дистанционное взаимодействие врача и пациента, а также проведение консилиумов и иную коммуникацию врачей с другими медицинскими специалистами. Среди главных услуг в форме телемедицины эксперты выделяют консультации у врача, дистанционный мониторинг здоровья, получение второго мнения, профилактику симптомов и возможных болезней.

В АВАНГАРДЕ НОВОГО РЫНКА Среди ключевых игроков на рынке медицинских онлайн-консультаций эксперты выделяют такие компании, как «Сберздоровье», «Доктор рядом», «Доктис», BestDoctor. В первом квартале 2023 года, согласно исследованию Smart Ranking, объем выручки компаний, занимающихся телемедициной, составил 3,142 млрд рублей, продемонстрировав рост на 48% в сравнении с первым кварталом 2022 года.

По словам Максима Чернина, председателя Академического совета программы «Управление бизнесом» Высшей школы бизнеса НИУ ВШЭ, председателя совета директоров МК «Доктор рядом», необходимо учитывать, что эта цифра включает себя услуги не только классической телемедицины, но и объемы существенно выросшего за последние годы направления дистанционных услуг по психологии и психотерапии. В целом существенных изменений в структуре спроса и предложения в первом полугодии на рынке не произошло: телемедицина практически уже стала стандартом наполнения программ ДМС в корпоративных программах, все чаще соцпакеты корпоративных клиентов дополняются уже упомянутой телепсихологией (всплеск спроса на которую произошел в 2022 году), некоторые клиники стараются внедрить дистанционные консультации в стандартный процесс обслуживания своих пациентов, хотя до ярких масштабных результатов тут еще далеко.

Как отмечает Игорь Башков, коммерческий директор компании «Нетрика Медицина» (входит в N3.group и ГК «Ташир Медика»), в общественном сознании телемедицина понимается пока почти исключительно как общение врача и пациента по видеосвязи, хотя на практике она включает широкий круг дистанционных взаимодействий внутри системы здравоохранения. «Самый распространенный сегодня вариант взаимодействия в госсегменте — телемедицинская консультация „врач — врач“. Такие консультации позволяют проводить консилиумы для „сложных“ пациентов, получать второе мнение, принимать решения о маршрутизации больных», — поясняет он.

По словам Александра Солонина, генерально-го директора Ассоциации частных клиник Санкт-Петербурга, основные тенденции рынка телемедицины связаны прежде всего с возрастающими потребностями пациентов в использовании удобных цифровых технологий. «Сегодня важно учесть интересы пациента, который приобретает большие возможности от удаленной консультации и мониторинга состояния здоровья независимо от своего места нахождения. Медицинская организация в то же время



В РОССИИ ПРИ ОБЩЕМ КОЛИЧЕСТВЕ ОЧНЫХ ПОСЕЩЕНИЙ ВРАЧА ОКОЛО 2 МЛРД В ГОД ДОЛЯ ДИСТАНЦИОННЫХ КОНСУЛЬТАЦИЙ НЕ ПРЕВЫШАЕТ 2–3%

может снизить пики в загрузке своих врачей, повысить доступность для пациентов в высококвалифицированном персонале, в том числе как второе мнение. А со стороны регуляторов стоит задача снизить риски некачественной медицинской помощи, то есть обеспечить безопасность пациента при использовании телемедицинских технологий», — рассуждает господин Солонин.

РОССИЙСКИЙ ОПЫТ По словам экспертов, в сравнении с крупными западными рынками и, например, с рынком Китая телемедицина формата «врач — пациент» в России развита пока довольно слабо. «Так, например, в 2021 году в США количество удаленных консультаций превысило количество очных приемов (на пике борьбы с ковидом), в Китае на несколько лидеров медтех-рынка приходится около 800 млн пациентов. В России при общем количестве очных посещений врача (около 2 млрд в год) доля дистанционных консультаций не превышает 2–3%», — приводит данные господин Чернин.

У этой статистики, по мнению эксперта, целый ряд причин. Во-первых, существенные законодательные ограничения услуги: невозможность постановки диагноза без проведения очного приема, назначения терапии и лекарственных препаратов, оформления и закрытия больничного листа. На вышеупомянутых рынках этих ограничений либо давно нет, либо они были сняты в разгар пандемии. Во-вторых, более 85% населения РФ обслуживается в системе ОМС, в государственных учреждениях, а не в частных клиниках или в рамках ДМС-программ. А указанные выше ограничения пока не позволяют интегрировать

технологии в государственную систему, так как это потребует существенного увеличения ресурсов. «В-третьих, медицина — весьма консервативная отрасль, в отличие от ритейла или банкинга, любые изменения внедряются здесь гораздо медленнее, в соответствии с принципом „не навреди“, да и специалисты в области цифровых технологий гораздо охотнее устраиваются на работу в банки или технологические экосистемы», — отмечает господин Чернин.

При этом, по словам господина Солонина, развитие формата телемедицины несет в себе не только положительные медицинские и социальные эффекты для отрасли здравоохранения, но и существенные экономические выгоды. «Сейчас в решении врачей при постановке диагноза доля инструментальных и лабораторных исследований составляет более 90%, а эффективность телемедицинских консультаций в 80% случаях не отличается от очных. Интеллектуальные компетенции врачей легко и эффективно используются дистанционно, когда не требуется мануальная и инструментальная диагностика и лечение. Таким образом, дистанционная коммуникация „врач — пациент“ и „врач — врач“ значительно сокращает затраты, в том числе и на перемещение и транспорт», — обращает внимание эксперт.

Также снижение потоков пациентов в медицинские организации значительно сократит затраты на избыточные мощности при капитальных вложениях и операционные расходы. По некоторым оценкам, снижение может составить до 20–30%. Еще один экономический эффект от телемедицины лежит в плоскости временных затрат персонала на предварительный сбор данных и жалоб пациента. За счет

дистанционного предварительного анкетирования, согласно данным хронометражных исследований, в амбулаторном звене экономия составляет около 20%.

Одной из главных проблем, по мнению господина Солонина, в отрасли здравоохранения является дефицит кадров, и внедрение телемедицины может также существенно повлиять на количество необходимых специалистов в штатном расписании медицинской организации, когда дистанционно могут привлекаться недозагруженные врачи из других организаций и даже регионов.

«Также нужно отметить важную роль телемедицины при трансформации модели здравоохранения за счет цифровизации при переходе к превентивной и профилактической медицине. Амбулаторное звено в этой модели будет заниматься не столько лечением и сохранением здоровья заболевших, сколько формированием здоровья с учетом персонализированных данных пациента. Такое сопровождение и мониторинг эффективно делать в дистанционном формате, в чем, собственно, и видят свое преимущество многие частные клиники, которые укрепляют доверие своих пациентов, в том числе за счет применения новых телемедицинских технологий», — рассуждает эксперт.

По мнению господина Чернина, ключевым преимуществом телемедицинской технологии является возможность оперативной связи с квалифицированным медицинским специалистом практически в любое время и из любой точки страны и мира. И если для жителя крупного города это экономит прежде всего его время, то для жителей небольших населенных пунктов и особенно удаленных территорий зачастую это существенно повышает шансы на получение профессиональной консультации нужного врача даже редкой специализации. Помимо географических, телемедицина частично снижает и финансовые барьеры: как правило, цена на дистанционные консультации несколько ниже стоимости очного приема. Кроме того, для многих людей визит к врачу — это еще и психологический вызов, для этого нужно морально собраться, тогда как связаться с врачом по видео- или аудиосвязи — гораздо проще. Все это не только повышает удобство для пациента, но и способствует более раннему выявлению заболевания и началу лечения, что критически важно для его успешности.

«Что касается недостатков, то основной из них — законодательные ограничения, в силу которых услуга телемедицины пока еще не может считаться целостной и законченной. Но и в этом вопросе есть подвижки: так, с 1 августа правительство РФ установило Экспериментальный правовой режим (ЭПР) для пациентов 15 медицинских учреждений, в число которых вошли такие компании, как „Медси“, „СберЗдоровье“, „Доктор рядом“, „Ниармедик“, „РЖД-медицина“. В соответствии с этим режимом после очного первичного приема пациент может проходить наблюдение и консультации в удаленном формате в том же медицинском учреждении, но у любого другого врача данной клиники, а специалист вправе корректировать диагноз, назначать терапию и выписывать онлайн-рецепты. Это говорит о намерении государства шаг за шагом смягчать законодательство и делать медицину более доступной для граждан», — заключает господин Чернин. ■

РОМАН ДЗВИНКО: «ИМПОРТОЗАМЕЩЕНИЕ В IT И ЛИЦЕНЗИОННЫЙ ШАНТАЖ РОССИЙСКОГО БИЗНЕСА»

Российские компании сегодня активно ищут замену иностранному программному обеспечению среди отечественных вендоров. Ведущие позиции занимают IT-компании, начавшие разрабатывать аналоги западных решений еще до санкций. Об импортозамещении программных решений в России, а также о том, почему нежелательно легализовать пиратское ПО, Business Guide побеседовал с исполнительным директором НПЦ «БизнесАвтоматика» Романом Дзвинко.

BUSINESS GUIDE: Какова нынешняя ситуация на IT-рынке в России в части использования западного софта? Какие риски несут компании, использующие нелегальное программное обеспечение?

РОМАН ДЗВИНКО: Большинство компаний в России продолжают использовать западный софт либо нелегально, либо полужакоально, что связано с необходимостью обхода иностранных санкций и поиска различных механизмов покупки лицензий. Ранее компании имели возможность продлевать лицензии на западное ПО, но с этой осени продление стало недоступным. Кроме того, возникла проблема лицензионного шантажа со стороны ушедших вендоров. Это создает риск для российских компаний, так как в случае отзыва лицензий вся их инфраструктура может перестать функционировать, что приведет к полной парализации системы, основанной на западном софте. Большие промышленные предприятия и холдинги могут потерять все в один день после отзыва лицензий как аппаратной, так и программной инфраструктуры.

Мы находимся в ситуации, когда легально импортные лицензии не купить, а продлевать текущие нет возможности. Исходя из этого, если в 2023–2024 годах компания хочет быть уверенной в том, что ее деятельность не остановится в любой момент, необходимо вкладываться в собственную независимую инфраструктуру и отечественное ПО. Это позволит обеспечить функциональность внутренних процессов и поможет создать крепкий фундамент с перспективой для будущего.

BG: В мае прошли слухи о возможной легализации пиратского ПО. Как вы к этому относитесь?

РОМАН ДЗВИНКО: Это нивелировало бы весь многолетний вклад в развитие отечественных технологий и нанесло бы колоссальный ущерб на уровне всех секторов экономики. Безусловно, для участников IT-рынка принятие подобных мер могло бы обернуться потерей сотни миллионов рублей. С высокой степенью вероятности это привело бы к полному исчезновению доли российского программного обеспечения и услуг в коммерческом секторе ввиду неравных условий конкуренции со стороны бесплатного или более дешевого пиратского ПО.

Стремление компаний к экономии за счет использования нелегальных программных продуктов подвергает риску как сам бизнес, так и простых пользователей. Среди негативных последствий — вероятность заражения компьютерной сети предприятия и утечка персональных данных пользователей.

В текущем году зафиксировано резкое увеличение количества масштабных утечек данных у российских компаний. В связи с этим принимаются новые поправки в законодательство, например, в сентябре кабмин поддержал введение оборотных штрафов за повторную утечку персональных данных.

BG: Вы думаете, иностранные вендоры отслеживают использование своего ПО?

РОМАН ДЗВИНКО: Есть мнение, что иностранные вендоры не заинтересованы в соблюдении санкционной политики США в отношении России, по слухам, даже сами



НПЦ «БИЗНЕСАВТОМАТИКА»

предлагают продлевать подписку крупным организациям. В апреле Microsoft был оштрафован на \$3 млн за продажу программного обеспечения российским фирмам, попавшим под санкции. Согласно уведомлению OFAC, штрафы были наложены в связи с тем, что Microsoft не смог проконтролировать процесс «перепродажи» ПО и услуг компании через сторонних партнеров. Крупным иностранным вендорам невыгодно продолжать работать в России под таким напором, учитывая, что для многих компаний наш рынок не является крупным. Например, доля выручки немецкого производителя SAP в России и СНГ в 2022 году составляла всего 1,7% его мирового дохода.

BG: Какие возможности открываются перед российскими IT-компаниями в связи с растущим спросом на импортозамещение решений? Как изменения на рынке заказной разработки повлияли на процессы в вашей компании?

РОМАН ДЗВИНКО: Компании активно ищут замену иностранным программным решениям среди отечественных вендоров специализированной разработки ПО. Те, у кого нет возможности на покупку защищенных, аттестованных enterprise-решений, стремятся оптимизировать свои ресурсы, переходя в облака, жертвуя частью функционала.

Крупный бизнес не может рисковать своей эффективностью, поэтому все чаще обращается к заказной разработке. Мы системообразующее предприятие, нашими основными заказчиками выступают госсектор, но за последний год у нас значительно возросло количество и коммерческих проектов: примерно на 20%. Основной спрос идет на замещение импортных продуктов и услуг, таких как системы бизнес-аналитики, No-code-платформы, системы управления проектами и другие.

Наши решения остаются одними из ведущих на рынке российского ПО благодаря тому, что долгое время мы сосуществовали в жестких конкурентных условиях с иностран-

ными вендорами. Мы основываемся на западных методологиях и разрабатываем продукты, которые адаптированы под отечественную специфику без потери функционала. В результате заказчик получает продукт, превосходящий западные аналоги по качеству, эргономике, инструментарию и многим другим факторам.

BG: Ваша компания — отечественный пионер внедрения технологии No-code. Расскажите о ее специфике.

РОМАН ДЗВИНКО: С появлением No-code практически вся разработка систем для автоматизации предприятий происходит на «кончиках пальцев» аналитиков. Современные платформы, в том числе наша No-code-платформа Visary, обладают широкими возможностями настройки, что существенно сокращает сроки реализации проектов, при этом позволяет соблюдать критерии по отказоустойчивости и надежности систем.

BG: Какие продукты и услуги в настоящее время наиболее востребованы на рынке?

РОМАН ДЗВИНКО: Несмотря на то, что наша компания в основном специализируется на заказной разработке, мы получаем все больше заявок на замену иностранных облачных сервисов. В наше время облачные платформы становятся

все более популярными среди малого и среднего бизнеса в России. Переход на них позволяет им сэкономить ресурсы и избежать необходимости приобретения дорогостоящего оборудования.

Исследования показывают, что уже к 2025 году 85% компаний планируют перейти на SaaS-технологии, а 55% компаний уже используют облака для размещения своих IT-систем. Раньше многие предпочитали популярные иностранные сервисы, такие как Jira, Power BI. Но теперь этих сервисов нет, а существующие российские решения не соответствуют требованиям современного бизнеса.

BG: Какая стратегия у компании по развитию IT-решений?

РОМАН ДЗВИНКО: В связи с растущим запросом на импортозамещение облачных сервисов мы приняли коллегиальное решение о разработке собственной облачной платформы под названием Visary Cloud. Это будет не просто замена иностранным сервисам, а инновационный продукт, которого еще не было на российском рынке облачных услуг. В основу сервиса лягут наши зрелые промышленные решения, уже зарекомендовавшие себя среди крупных клиентов. Мы уже определили «дорожную карту», в рамках которой будут постепенно внедряться обновления существующих и выпускаться новые модули Visary, а также будет происходить их последующий перенос в облачные версии. Более того, облачные модули также будут содержать No-code-компонент для быстрой настройки системы под специфику заказчика.

В ходе модернизации мы уже обновили и расширили функциональность системы управления бизнес-процессами Visary BPM и аналитической платформы Visary BI, а также вывели на рынок новый модуль по управлению задачами Visary Tracker.

ВАСИЛИСА МОТОВА

На правах рекламы



ЕВГЕНИЙ ПЛАВЕНКО

К началу августа 2023 года в Минцифры РФ отчитались, что доля отечественных продуктов для информационной безопасности достигла 90%, по итогам 2022 года этот показатель доходил до 70%

По словам эксперта Института кибербезопасности и защиты информации Политеха Анны Селивановой, Россию покинуло свыше 100 зарубежных производителей систем кибербезопасности. «С февраля 2022 года страна стала, пожалуй, одной из самых атакуемых киберпреступниками стран мира», — констатирует госпожа Селиванова.

«Последние полтора года побили все рекорды по количеству кибератак на российские сайты», — подтверждает генеральный директор агентства DOT Глеб Иванюшкин. — Контроля исключительно внутри организации становится недостаточно. Многие наши клиенты сформировали новые отделы по информационной безопасности, частично делегировав вопросы защиты интернет-проектов диджитал-агентствам».

Среди делегируемых задач он назвал аудит внедренных систем кибербезопасности, обновление лицензий CMS «Битрикс», отслеживание свежих версий серверного ПО, свободных от ошибок и более устойчивых к взлому. «Это можно назвать созданием бастиона первичной защиты от атак DDoS», — говорит господин Иванюшкин.

К началу августа 2023 года в Минцифры РФ отчитались, что доля отечественных продуктов для информационной безопасности (ИБ) достигла 90% (для сравнения, по итогам 2022 года этот показатель доходил до 70%). Рынок российских разработок в сфере ИБ в 2022 году Центр стратегических разработок при правительстве РФ (ЦСР) оценил в 193,3 млрд рублей (+4% к 2021 году). В ЦСР прогнозируют, что к 2027 году его емкость достигнет 559 млрд при росте на 24% в среднем ежегодно. Интерес к решениям кибербезопасности отметили и на рынке IT-стартапов: по данным центра инноваций и инвестиций MTS StartUp Hub, в первом полугодии 2023 года стартапы в сфере ИБ вошли в топ-3 (6% от общего числа стартапов), при этом их количество удвоилось относительно 2022 года.

В ГК «Финам» оценили текущий оборот компаний, работающих на российском рынке кибербезопасности, в 220–230 млрд рублей. «Выручка лидирующих компаний уже сейчас растет почти вдвое за год: темпы прироста составляют 100%. Вполне вероятно сохранение таких темпов в течение двух-трех лет», — комментирует аналитик ГК «Финам» Леонид Делицин.

«Рынок ИБ сильно сегментирован. Сегментация происходит не только по заказчикам (b2b, b2c, b2g), но и по классам средств защиты информации: антивирусы, межсетевые экраны, защиты от несанкционированного доступа (НСД), утечек и т. д.», — говорит руководитель центра комплексной безопасности компании «Ланит» Дмитрий Дудко.

Лидерами рынка среди отечественных вендоров в сфере ИБ (в разных сегментах защиты) являются «Лаборатория Касперского», Positive Technologies, Dr.Web, BI.ZONE, «Ростелеком-Солар», «КриптоПро», «Код безопасности», Innostage, Angara Security.

КОМПАНИИ МЕНЯЮТ КИБЕРЩИТ

ЭКСПЕРТЫ ОТМЕЧАЮТ РОСТ ОТЕЧЕСТВЕННОГО РЫНКА РЕШЕНИЙ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВО ВСЕХ СЕГМЕНТАХ — СЕГОДНЯ РЕЧЬ ИДЕТ О 90% РОССИЙСКИХ РАЗРАБОТОК НА ПРЕДПРИЯТИЯХ СТРАНЫ. ВЫРУЧКА КОМПАНИЙ, РАБОТАЮЩИХ НА РЫНКЕ КИБЕРБЕЗОПАСНОСТИ, УДВОИЛАСЬ И ДОСТИГЛА 220–230 МЛРД РУБЛЕЙ. РАЗВИТИЕ СЕГМЕНТА СВЯЗЫВАЮТ С УСИЛЕНИЕМ КИБЕРАТАК НА ФОНЕ САНКЦИЙ И УХОДА ЗАПАДНЫХ РАЗРАБОТЧИКОВ. СРАВНИТЕЛЬНО НОВЫЙ ТРЕНД — АТАКИ НА ПРОМЫШЛЕННЫЕ ПРЕДПРИЯТИЯ, КОТОРЫМ ПОТРЕБОВАЛАСЬ СРОЧНАЯ ЗАЩИТА КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ.

ОЛЬГА ГОЛОВИНА

КИБЕРБЕЗОПАСНОСТЬ С ГОСПОД-ДЕРЖКОЙ

Несмотря на дефицит бюджета в несколько триллионов рублей, государство готово тратить деньги на кибербезопасность. Вероятно, поэтому в 2023 году расходы на федеральный проект «Информационная безопасность» (входит в нацпрограмму «Цифровая экономика», действующую с 2019 года) в 2023 году увеличили более чем на 7%, до 7,9 млрд рублей, в то время как в целом расходы на другие проекты цифровой нацпрограммы урезали на 35%.

Дотации, в том числе разработчикам решений по ИБ, выделяют Российский фонд развития информационных технологий (РФРИТ), «Сколково», Фонд содействия инновациям (ФСИ). На базе Фонда развития интернет-инициатив (ФРИИ) создали акселератор, где инвестируют в IT-стартапы (размер грантов — от 5 до 65 млн рублей, общий размер финансирования на ближайшие годы — по 750 млн в год). ФРИИ финансирует разработчиков решений в сфере криптографии, борьбы с вирусными или DDoS-атаками, защиты от мошенничества.

Кроме денежной поддержки кибербезопасности, разработчиков касаются все стандартные пакеты поддержки IT, включая сниженные страховые тарифы, льготные кредиты, льготную ипотеку, отсрочку от призыва на военную службу.

ПЕТЕРБУРГСКИЙ СЕГМЕНТ

Всего, по оценкам экспертов, в Петербурге работает около 300 предприятий, оказывающих услуги в сфере кибербезопасности (включая офисы федеральных игроков). Самый заметный производитель решений в области ИБ — компания «Конфидент» (разрабатывает средства защиты от несанкционированного доступа, защиты виртуальной инфраструктуры и централизованного управления безопасностью). Также ИБ-системы, в том числе для производственных предприятий, производит «Ланит-Терком» (входит в ГК «Ланит»).

Совокупную выручку производителей ИБ-решений из Петербурга и Ленобласти господин Делицин оценивает примерно в 11 млрд рублей (где 9 млрд приходится на Петербург и 2 млрд — на Ленобласть). «Рынок кибербезопасности сильно фрагментирован, и даже доля крупных игроков, как правило, не превышает 5%», — сообщил эксперт. Господин Дудко считает, что оценивать рыночную долю петербургских компаний следует по классам средств защиты. «В таких сегментах, как защита виртуализации и защита от НСД, доля компаний Петербурга приближается к 50%», — подсчитал он.

Предприятия Петербурга и Ленобласти идут в фарватере федерального тренда в сфере ИБ из-за роста числа кибератак. «Мы наблюдаем увеличение спроса на услуги в области информационной безопасности», — делится региональный представитель компании NGR Softlab Андрей Личман. — По нашим оценкам, он составляет 20–25% в год. В ближайшие годы этот темп сохранится».

«Если раньше покупали в основном только антивирус и средства межсетевого экранирования, то сейчас растет спрос и на анализаторы трафика, средства обнаружения атак, средства защиты рабочих станций. Пользуются определенным спросом и системы мониторинга событий, оркестрации (управления сложными компьютерными системами)», — сообщили изданию в пресс-службе правительства Ленинградской области.

В руководстве региона отметили рост затрат организаций на ИБ в диапазоне 15–20%. Среди самых востребованных решений — высокопроизводительные межсетевые экраны (NGFW) и межсетевые экраны уровня приложений (WAF).

ПРОМЫШЛЕННОСТЬ ПОД УГРОЗОЙ

По словам госпожи Селивановой, в последнее время возросло число атак именно на промышленный сегмент. «Раньше в основном от кибератак защищались корпоративные компании, а в последнее время участились атаки на производственные корпорации. Соответственно, эти компании тоже начали серьезно заниматься безопасностью», — описала ситуацию эксперт.

О трендах к защите производств говорят и в «Лаборатории Касперского». Эксперт по кибербезопасности Kaspersky ICS CERT Владимир Дашенко обращает внимание, что одна из ведущих тенденций в сфере цифровизации предприятий — защита сегмента облачных технологий (OT-сегмент), поскольку технологическая инфраструктура все больше подключается к интернету. «Только во втором полугодии 2022 выросла доля компьютеров автоматизированных систем управления (АСУ), на которых блокировались попытки атак вредоносными объектами из интернета: она увеличилась на 12 п. п. по сравнению с первым полугодием. Из-за этих факторов промышленные организации проявляют больший интерес к специализированным защитным решениям от киберугроз, которые учитывают специфику эксплуатируемых систем, долгий цикл использования оборудования и устаревших версий операционных систем, а также исключают воздействие на производительность и функциональную безопасность АСУ ТП», — комментирует господин Дашенко.

Эксперт уверен, что такие отрасли, как логистика, металлургия, тяжелое машиностроение и другие крупные игроки, будут продолжать активно интегрировать цифровые решения в производственные процессы, но внедрение потенциально увеличивает площадь поверхности кибератаки, а потому решения в сфере ИБ необходимы.

Его слова подтверждают и данные Cdo2day (ресурс АНО «Цифровая экономика», проект Минцифры): в ближайшие три года основная доля IT-затрат производственных предприятий РФ придется на кибербезопас-

ность (затраты на промышленную «цифру» в 2022 году составили около 600 млрд рублей).

«УДАЛЕНЩИКИ» НА ОСТРИЕ АТАКИ

Развитие интернет-среды перевело многие бизнес-процессы, включая работу с подрядчиками на удаленку. «Предоставление доступа к ресурсам компании, в том числе довольно широких прав к критически важным системам, для сотрудников подрядных организаций, внешних специалистов и консультантов стало сегодня стандартной практикой», — обращают внимание в компании «Ростелеком-Солар». Это выявило и новые риски.

«Атаки, реализуемые через поставщиков, в том числе IT-подрядчиков, являются наиболее рискованными для предприятий критической информационной инфраструктуры. Злоумышленники могут получить доступ к инфраструктуре компаний, воспользовавшись уязвимостями в системе информационной безопасности своих партнеров», — поясняет заместитель генерального директора Angara Security Руслан Косарим.

По словам киберэксперта компании «Код безопасности» Павла Коростелева, если у предприятия нет механизмов безопасного удаленного доступа, «злоумышленник может скомпрометировать „учетку“ легитимного пользователя, а затем украсть конфиденциальную информацию, удалить ее или начать распространять по сети. Также хакер может взломать систему и опять же получить доступ к внутренней сети». «Для взлома достаточно скомпрометировать от двух до пяти учетных записей, чтобы получить доступ к критичным цифровым активам», — раскрыл механику взлома господин Косарим. ■

Тематическое приложение к газете «Коммерсантъ» (онлайн-выпуск Санкт-Петербург, Business Guide «Цифровая экономика»)

Владимир Желонкин — генеральный директор АО «Коммерсантъ», главный редактор
Анатолий Гусев — автор дизайн-макета
Андрей Ершов — главный редактор СПб страниц
Александр Коряков — бильд-редактор
Валерий Грибанов — выпускающий редактор
Марина Шевченко — корректор
Василиса Сатирская — верстка
Марина Победенная — рекламная служба

Адрес редакции и издателя: 123112, г. Москва, Пресненская наб., д. 10 этаж 35. Тел. (495) 797-6970. Адрес редакции в Санкт-Петербурге: 191024, Харьковская ул., д. 8А, лит А. Тел. (812) 324-6949

Учредитель: АО «Коммерсантъ». Тематическое приложение к газете «Коммерсантъ», зарегистрировано Роскомнадзором, регистрационный номер и дата принятия решения о регистрации ПИ №ФС77-76923 от 11.10.2019 года

В печатном виде номер не выходит. Распространяется бесплатно. 16+

Графика на обложке: Арсений Блинов



БУДЬ В КОНТАКТЕ



ПОДПИШИСЬ И ВЫИГРАЙ ПРИЗ
ОТ ИЗДАТЕЛЬСКОГО ДОМА «КОММЕРСАНТЪ»

Группа «Коммерсантъ» Санкт-Петербург
во «ВКонтакте» это:

- АКТУАЛЬНЫЕ НОВОСТИ
- ОБЪЕКТИВНЫЙ АНАЛИЗ
- ЭКСКЛЮЗИВНЫЕ КОММЕНТАРИИ О ВАЖНЕЙШИХ СОБЫТИЯХ И ТРЕНДАХ
- РЕГУЛЯРНЫЕ РОЗЫГРЫШИ БИЛЕТОВ НА КОНЦЕРТЫ, СПЕКТАКЛИ И ДРУГИЕ МЕРОПРИЯТИЯ



ПЕТЕРБУРГ

Истории бизнеса

СПЕЦИАЛЬНЫЙ ПРОЕКТ
«ПЕТЕРБУРГЪ. ИСТОРИИ БИЗНЕСА»
О ВКЛАДЕ КОМПАНИЙ
В РАЗВИТИЕ СЕВЕРНОЙ СТОЛИЦЫ



Ответственные предприниматели заботятся не только об увеличении доходности своих компаний, но и о том, какой позитивный след они оставят в богатой истории нашего города